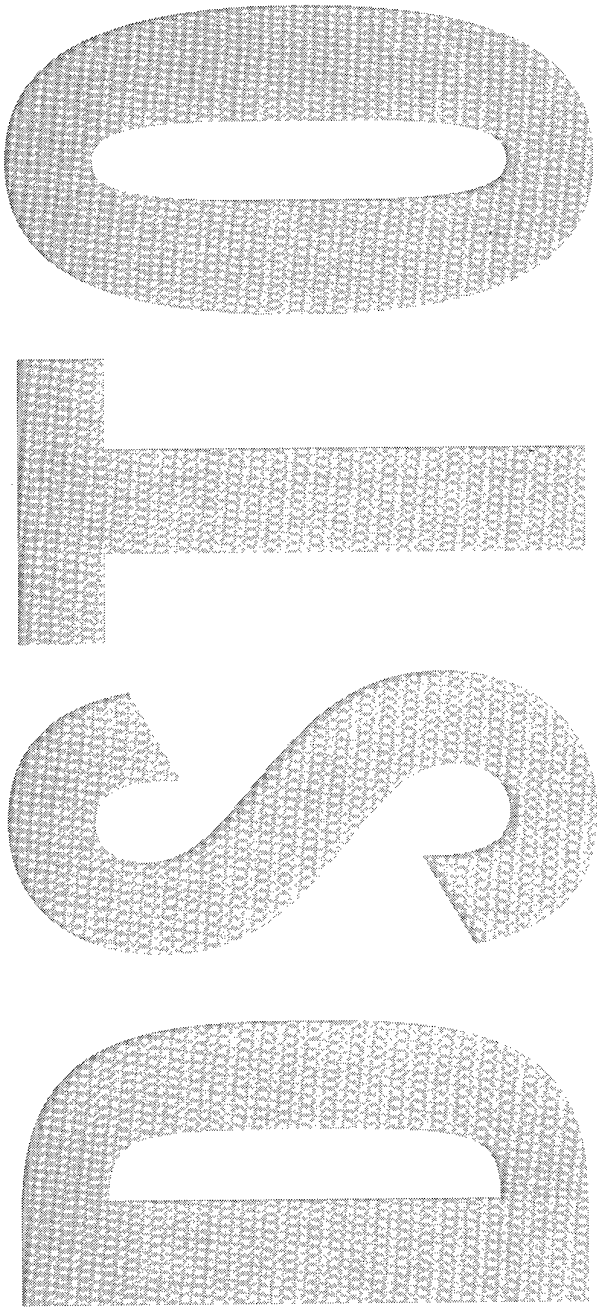
DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO



# Military Information Operations Analysis Using Influence Diagrams And Coloured Petri Nets

R. J. Staker

DSTO-TR-0914

# Military Information Operations Analysis Using Influence Diagrams And Coloured Petri Nets

*R. J. Staker*

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO–TR–0914

## ABSTRACT

This report describes how Influence Diagrams, Coloured Petri Net models and related techniques may be used to analyse certain aspects of Military Information Operations. An example is employed to demonstrate these techniques. The example used is a very simplified representation of a Military Command Organisation dealing with a decision problem.

The objective of the report is to provide theory, methods and techniques to support the assessment of the effect of Military Information Operations on such organisations. The simplicity of the example permits the basic concepts to be clearly conveyed. They may readily be extended to the analysis of more complex examples as required.

The most fundamental and significant concept developed in this report is that of a common quantitative measure of effectiveness that encompasses all types of Information Operations relevant to Information Warfare. This permits the direct comparison of the effectiveness of alternative Information Operation options with one another and also with conventional operations options. This latter ability is essential if Information Operations are to be employed appropriately as part of a broader range of military options.



*Published by*

*DSTO Electronics and Surveillance Research Laboratory*
*PO Box 1500*
*Salisbury, South Australia, Australia 5108*

*Telephone:* *(08) 8259 5555*
*Facsimile:* *(08) 8259 6567*


*AR No. AR–011–162*
*December, 1999*

***APPROVED FOR PUBLIC RELEASE***

# Military Information Operations Analysis Using Influence Diagrams And Coloured Petri Nets

## EXECUTIVE SUMMARY

This report describes how Influence Diagrams, Coloured Petri Net models and related techniques may be used to analyse certain aspects of Military Information Operations. An example is employed to facilitate the exposition of these techniques. The example used is a much simplified representation of a military command organisation. The objective of the report is to provide theory, methods and techniques to support the assessment of the effect of Military Information Operations on such organisations. The simplicity of the example permits the basic concepts to be clearly conveyed. They may readily be extended to the analysis of more complex examples as required.

The most fundamental and significant concept developed in this report is the introduction of a common quantitative measure of effectiveness that encompasses all types of Information Operations relevant to Information Warfare. This permits the direct comparison of the effectiveness of alternative Information Operation options. Furthermore, this effectiveness measure is also applicable to conventional operations, so that the effectiveness of Information Operations may be compared against the effectiveness of alternative conventional operations. This latter ability is essential if Information Operations are to be employed appropriately as part of a broader range of military options.

The focus of the report is on Information Operations *effects*. The means by which such effects might be achieved are not discussed in detail here. This will be a matter for future research. However, some commonly cited examples of such means are physical targeting of information repositories and information infrastructure, Electronic Warfare, Operational Security, Signature Reduction, Psychological Operations, disinformation, decoys, diversionary tactics and Computer Network Attack.

The effects have been classified into two broad categories, which have been termed *secular effects* and *temporal effects*. Secular effects are considered to be those effects which do not depend explicitly on a time parameter. Temporal effects, in contrast, do exhibit an explicit dependence on a time parameter. The secular effects that are considered in this report are *Information Denial*, *Deception* and *Psychological Attitude Shift*. The temporal effects considered are *Information Delay* and *Prolonged Decision Making*. These last two are obviously characterised by the temporal parameters of delay time and increase in decision-making time, respectively.

It is felt that these five effects broadly cover all aspects of Information Warfare, and that, therefore, the techniques presented in this report provide are applicable to all Information Warfare problems of interest. They do not, however, cover the entire field of Information Operations. For example, they do not address the effect of Information Exploitation. These wider effects will also be a matter for future research.

The most important achievement reported here has been the quantification of all five effects in terms of a common measure. The significance of this is that it allows the numerical comparison of the effectiveness of Information Operations of differing types. This

in turn allows the most effective type of operation to be selected by a commander. Furthermore, the effectiveness of conventional operations could also, in principle, be reduced to the same measure, thus permitting a comparison of the effectiveness of Information Operations with that of comparable conventional operations. This would be important in justifying the allocation of valuable resources to Information Operations.

The analysis methods and techniques demonstrated are Information Theory, Utility Theory, Decision Trees, Influence Diagrams, Coloured Petri Nets, Monte Carlo Simulation and Queueing Network Analysis. Information Theory is used to measure information quantity, while Utility Theory is used to measure information importance and significance. Decision Trees and Influence Diagrams are alternative techniques for solving decision problems based on Utility Theory. Influence Diagrams are the more recently invented and more powerful technique. While the preceding methods are sufficient for analysing secular effects, they do not encompass temporal effects. Coloured Petri Nets are therefore used to include temporal effects in the model. Two means of deriving the required measure of effectiveness from the Coloured Petri Net are demonstrated. The first is Monte Carlo Simulation, which is generally applicable, but can be computationally expensive if accurate results are required. The second is reduction of the Coloured Petri Net to a Queueing Network. For sufficiently elementary problems, the Queueing Network can be solved mathematically for the required effectiveness measures. This approach is also demonstrated for the simple example used here.

# Contents

# Figures

# Tables

# Glossary

**BBN** Bayesian Belief Network

**C3I** Command, Control, Communications and Intelligence

**CPN** Coloured Petri Net

**CPU** Central Processing Unit

**DICE** Distributed Interactive C3I Effectiveness (Tool)

**EVPI** Expected Value of Perfect Information

**INTELO** Intelligence Organisation

**IO** Information Operations

**IW** Information Warfare

**MIO** Military Information Operations

**US** United States

# 1 Introduction

This report describes how Influence Diagrams, Coloured Petri Models and related modelling techniques may be used to analyse certain aspects of Military Information Operations. An example is used to demonstrate the ideas involved. This example is intended to be a much simplified representation of a military command organisation dealing with a decision problem. Information Operations are divided into five classes, according to the effects that they produce. These five classes are then divided into two broader classes according to whether the effect they produce explicitly depends on a time related parameter or otherwise. The last dichotomy dictates the form which the analysis must take.

The objective is to provide a general tool which permits the assessment of the impact of Military Information Operations on Military Command Organisations, and which allows the effectiveness of various Information Operation options to be compared. In the course of developing suitable methods, measures for the quantity, quality and value of information are proposed. It will be shown that the effectiveness of all five classes of Information Operation can be measured on a common quantitative scale. This allows the direct comparison of Information Operation options. Furthermore, the effectiveness of conventional operations can potentially be reduced to the same scale, thus permitting the direct comparison of the effectiveness of Information Operations with that of conventional operations. This ability is essential if Information Operations are to be employed appropriately as part of a broader range of military options.

## 1.1 Military Information Operations

The Military Information Operations (MIO) problem that is addressed by this report is that of analysing the susceptibility of military decision-making organisations to information-based attacks. The ability to be accurately able to perform such analyses will provide a basis for designing organisations which are robust against information-based attacks, hence contributing to defense against Information Operations. It will also assist in developing MIO strategies and tactics.

This report addresses some limited aspects of the problem. A general solution would be extremely complicated and therefore provide little clear insight into identifying what the crucial design considerations might be. By working on a restricted problem, the analysis remains tractable. Aspects not covered by the restricted problem addressed here may be studied by other means, perhaps using other techniques that are better adapted to their particular requirements. Once this is done, some synthesis of the understanding gained through the separate analyses will need to be done in order to achieve an overall understanding of the general problem.

Note that the term used in the opening paragraph of this section is *susceptibility*. For the purposes of this report, susceptibility is considered to be composed of two components. These are: the extent to which the decision-making organisation contains vulnerabilities to information-based attack; and, counterbalancing this, the extent and effectiveness of protective measures and countermeasures, which may partly protect these vulnerabilities from exploitation by an adversary. Determining susceptibility is only one aspect of the more general problem of determining the *risks* that might be posed by information-based

attacks. Some other aspects of the more general risk problem concern whether an adversary exists with the opportunity, capability and intent to exploit some vulnerability. The latter aspects of the general problem are not addressed in the present report.

The analysis here is further restricted by limiting the measures in terms of which the susceptibility is evaluated. Some measures which might be applicable are: the increase in the time required to make a decision; the decrease in quality of decisions made; and, the increase in the staffing level required to sustain a particular decision-rate. The last measure is supposed to relate to the ability of an adversary to create confusion through the use of deception, decoys and the like, thereby increasing the complexity of the decision problem.

An increase in the time required to make a decision is supposed to arise from the ability of an adversary to impede timely reception of the information required to make an informed decision. It may also arise in the case where the adversary employs confusion to increase the complexity of the decision-making problem and where an appropriate compensating manning level is not maintained. A decrease in decision quality is supposed to occur when some of the information that is required to make a properly informed decision has been denied or falsified by the adversary. Another way in which the quality of decisions may be affected is through the impact of psychological operations that affect the way in which decision alternatives are evaluated by the commander.

The relative quality of two decisions is determined by which is expected to yield consequences with the greater level of commander satisfaction in the absence of psychological operations. More will be said about how this may be determined later. The present report focuses on the first two measures listed above, which are decision-making time and decision quality.

Waltz [17, §1.5.2] provides a taxonomy of Information Warfare, originating from the US Air Force. From this he derives six offensive and defensive operation types: psychological operations, military deception, security measures, physical destruction, electronic warfare and information attack. The techniques developed in this report are relevant to all of these operation types.

## 1.2 Concepts used in Analysing Military Information Operations

The subsections below briefly describe some aspects of the theory of decision making, the measurement of information quantity, the measurement of information quality, modelling of temporal effects, and how these may be applied to analysing Military Information Operations.

### 1.2.1 Decision Making

For the purposes of this report, decision-making will be defined as the selection of one of a finite number of discrete alternative actions, which, based on the available information, would be expected to achieve the best possible consequence, according to some set of values or standards held by the decision-maker. In the example employed in this report,

the decision-maker is taken to be a military commander. Attention is focussed on rational, informed decision making. Deviations from rationality, due to human bias or resulting from physical or psychological stress, for example, have not been considered in this report, but could be included as part of subsequent research.

A well-developed mathematical theory, known as Decision Theory, has already been established for addressing problems concerning decision-making under uncertainty. Various aspects of this theory are described by von Neumann [16], Raiffa [12], Keeney [3] and Pearl[10, ch. 6], for example. It is a theorem of decision theory that, if certain axioms are satisfied, then a utility function $u(\cdot)$, which is a function of the outcomes space, $\mathcal{O}$, exists such that, for any two decision alternatives $A$ and $B$, with $A$ being considered to be preferable to $B$, the expected utility for action $A$ is strictly greater than the expected utility for action $B$, and that this function is unique up to a linear transformation. It is important to note that the decision-theoretic utility described here should not be confused with economic utility. The two are distinct concepts, as discussed by Keeney [3, §4.4.1].

The axioms alluded to above as being required for the existence of the utility function are referred to as the *axioms of consistent choice* or *axioms of utility theory.* One suitable set of axioms is given by Pearl [10, §6.1.4]. Similar sets of suitable axioms are given by von Neumann [16] and Raiffa [12].

In using the adjective *expected* in the definition of the utility, it has been implicitly acknowledged that the decision problem is of a probabilistic nature. Indeed, as discussed in reference [12, ch. 10], the concepts of utility and subjective probability are intimately intertwined.

Mathematically, for the case where the outcome random variable is discrete, the expected utility is given by

$$E\left[U|\cdot\right] = \sum_{i=1}^{n} P(\Omega = \omega_i \mid \cdot) u(\omega_i), \tag{1}$$

where $P(\Omega = \omega_i|\cdot)$ denotes the conditional probability of the outcome $\omega_i$ occurring when some particular, but here unspecified, condition holds, $n$ is the number of possible outcomes, $U = u(\Omega)$ is the utility random variable and $\Omega$ is the outcome random variable. When the outcome variable is continuous, the expected utility is given by

$$E\left[U|\cdot\right] = \int_{-\infty}^{\infty} u(\omega) f(\omega|\cdot) d\omega, \tag{2}$$

where $f(\omega|\cdot)$ is the distribution of $\omega$ for the specified condition.

The requirement that $u$ must satisfy in order to be a suitable utility function can be implicitly expressed as:

$$\exists u : A \succ B \Leftrightarrow E[U|A] > E[U|B], \tag{3}$$

where $A \succ B$ denotes that action $A$ is preferable to action $B$.

Often in analysing rational, informed decision making, risk neutrality is assumed. This means that the decision-maker is really only concerned with the expected utility of the decision, and is indifferent to the relative probabilities of the utility values. Such an assumption is only reasonable when the worst possible outcomes of individual decisions

are not disastrous. For example, it would be realistic in analysing economic problems where relatively small profits and losses are being considered. The utility function is then linear. On the other hand, when the stakes are high, responsible decision-makers tend to become more risk-averse. Risk aversion or risk propensity can be readily accommodated in the model, if required, by a suitable, non-linear but monotone, modification of the utility scale. The monotonicity requirement is imposed to ensure preservation of the preference ordering inherent in the utility function.

When the utility function $u(\omega)$ is continuous and twice differentiable, the local risk attitude function is given by $r(\omega) = u''(\omega)/u'(\omega)$, where primes have been used to indicate differentiation with respect to the variable $\omega$. It is negative for a risk-averse decision-maker, positive for a risk prone one and zero for one who is risk neutral. Risk aversion corresponds to a concave utility function, while risk propensity corresponds to a convex utility function. Utility functions having the same local risk attitude function are said to be *strategically equivalent.*

A simplifying assumption that can sometimes be made is one of constant risk attitude, i.e., $r(\omega) = K$. This subsumes the case of risk neutrality, which is simply that of zero risk aversion or propensity, i.e., $K = 0$. The reason for making such an assumption is that it simplifies the calculation of the value of information when there is a cost associated with obtaining the information. When the risk attitude function is constant, the cost of obtaining the information may be ignored, since in that case adding a constant to the outcome values results in the same constant being added to the expected value. The result is a linear transformation of the utility function, which is strategically equivalent to the utility function for the case of costless information. For further details concerning the role of risk attitude in decision theory, see Keeney [3, ch 4].

The risk attitude function is only definable when the utility scale corresponds to some tangible quantity, such as money, of which the decision-maker can, in principle, obtain some amount with certainty, and where the outcome space is continuous. When the utility scale being employed is an abstract one, and the outcome space is discrete rather than continuous, as is the case for a commander choosing one plan over another, the risk attitude function can not be employed. (See for example the situation described in Section 2.3.) However, it will be shown later in Section 2.8.3 that even in that case the utility function bears a relation to the commander's psychological attitude.

One common means of analysing a probabilistic decision problem, such as the one described above, is the use of a *Decision Tree.* Decision Trees are discussed in detail by Raiffa [12]. They are also described by Pearl [10, §6.2.1] and Neapolitan [8, §9.1]. Section 2.4 describes how the decision problem presented in Section 2.1 may be analysed using a Decision Tree. However, a more recent method for representing and analysing such decision problems employs Influence Diagrams (ID). These are described by Pearl [10, §6.2.3] and Neapolitan [8, §9.2]. Influence Diagrams are closely related to Bayesian Belief Networks (BBN), but whereas BBNs consist entirely of random variable nodes, Influence Diagrams also contain decision and utility nodes.

Influence Diagrams have the advantages over Decision Trees of providing a more concise graphical representation of the problem than do Decision Trees, and also of being able to be used more flexibly. Furthermore, since they employ BBNs for representing the conditional independence relationships between random variables, the efficient algorithms

used for computing the posterior marginal distributions for BBNs can also be advantageously applied to Influence Diagrams. Further illustration of some of the advantages of Influence Diagrams over Decision Trees is given by Matheson [6].

Section 2.5 describes how the decision problem presented in Section 2.1 may be represented as an Influence Diagram. Maxwell [7] describes the application of Influence Diagrams to another military problem. BBNs are discussed by Pearl [10, §2.2.5 and §3.3] and Neapolitan [8, ch. 5]. They have also been employed by the author elsewhere in the evaluation of information system network risk. See reference [15] for further details of this application.

### 1.2.2 Measuring Information Quantity

One of the foundations of scientific communications theory is C. Shannon's Information Theory [14]. This theory is concerned with quantifying the maximum "rate" at which information can be transmitted over a communication channel with given characteristics. This rate, termed the *channel capacity* and usually denoted by the symbol $C$, is essentially the proportion of the signal that may contain novel information for essentially error-free transmission. The remainder of the signal is composed of redundant information that allows errors or distortion introduced by the channel to be removed by the receiver.

The question arises as to what the terms "information source", "message", "transmitter", "channel", "receiver" and "destination" used by Shannon [14] correspond in the present context. The "information source" can be considered to be the region of interest to the commander. The "message" corresponds to events of military interest occurring in the region of interest. This message is transformed into a set of signals by the various sensors that are available. They may be highly technological or as simple as the eyes and ears of a reconnaissance team. The "transmitter" corresponds to these sensors. Before the signal reaches the decision-maker, in the final form of a report, several stages of interpretation may take place. It is assumed that the actual communication channels between the stages of interpretation are essentially error free, but that each act of interpretation may introduce some additional random errors, through misinterpretation. These interpretation stages and final reduction to report form correspond to the "channel" and the "receiver". Finally, the "destination" corresponds to the commander. This information flow is shown in block diagram form in Figure 1.

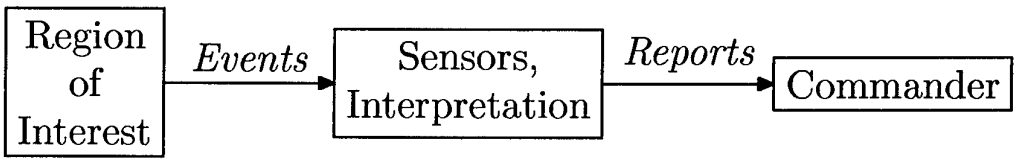



*Figure 1: Information Block Diagram*

The measure of information that lies at the foundation of Information Theory is *entropy*. The entropy of an information source measures the average amount of information contained in a message produced by the source in "binary digits" (bits), or more correctly in terms of "Hartleys" since it is not actually meaningful to speak of fractions of a bit, and entropy is a real number. An information source is represented as a random variable,

because, if it is not random, its value can be predicted and knowing its value provides no additional information. In consequence, deterministic information sources always have zero entropy.

In the present context, the term *informative random variable* will be used for the quantity reaching the destination, while the term *situational random variable* will be used for the quantity produced by the information source. In the definitions and results that follow, the symbol $X$ will be used to represent an informative random variable and the symbol $Y$ will be used to represent the corresponding situational random variable. It will be demonstrated that these play symmetrical roles in Information Theory.

The entropy of a discrete random variable $X$ is defined to be

$$\mathcal{H}(X) = -\sum_{x} \log_2 P(X = x) \cdot P(X = x), \tag{4}$$

where $P$ is the probability distribution of $X$. In this expression, the function $\log_2$ has greater precedence than multiplicative operations, consequently the argument of the logarithm function is just $P(X = x)$. The value of the logarithm is multiplied by the second occurrence of $P(X = x)$. This multiplication is indicated by a centred dot to emphasise that it applies to the value, rather than the argument, of the logarithm function.

The entropy of two discrete random variables $X$ and $Y$, considered jointly, is given by

$$\mathcal{H}(X, Y) = -\sum_{x,y} \log_2 P(X = x, Y = y) \cdot P(X = x, Y = y) \tag{5}$$

It follows from this definition that $\mathcal{H}(X, Y) = \mathcal{H}(Y, X)$.

The *mutual information* of $X$ and $Y$ is given by

$$\mathcal{I}(X, Y) = \mathcal{H}(X) + \mathcal{H}(Y) - \mathcal{H}(X, Y) \tag{6}$$

It follows from this definition that $\mathcal{I}(X, Y) = \mathcal{I}(Y, X)$. The mutual information of two random variables is a measure of how much information a knowledge of one of the random variable provides about the other. The *conditional entropy* of the random variable $Y$, given that the value of the random variable $X$ is known, is given by

$$\begin{aligned}
\mathcal{H}(Y|X) &= -\sum_{y,x} \log_2 P(Y = y|X = x) \cdot P(Y = y, X = x) \\
&= -\sum_{y,x} \left[\log_2 P(Y = y, X = x) - \log_2 P(X = x)\right] P(Y = y, X = x) \\
&= \mathcal{H}(Y, X) - \sum_{x} \log_2 P(X = x) \cdot \sum_{y} P(Y = y, X = x) \\
&= \mathcal{H}(Y, X) - \mathcal{H}(X)
\end{aligned} \tag{7}$$

Rearranging Equation 7 for $\mathcal{H}(Y, X)$ and substituting the result into Equation 6 gives:

$$\mathcal{I}(X, Y) = \mathcal{I}(Y, X) = \mathcal{H}(Y) - \mathcal{H}(Y|X). \tag{8}$$

This demonstrates that the mutual information is the decrease in entropy of the random variable $Y$ when the value of the random variable $X$ is known.

### 1.2.3 Measuring Information Value

This section discusses how a value may be associated with an information item derived from an information source. Many of the matters discussed here are also mentioned by Pearl [10, ch 6]. First, we should note that there may be various ways of valuing information. For example, *replacement cost* may be one measure that springs readily to mind. However, if there were no requirement for holding the information in the first place, there could be no value in replacing it. Instead, value will be assigned to information on the operational basis of the amount of extra value can be extracted from decisions that are made with the benefit of having the information concerned available.

To derive an appropriate value, the information item is regarded as a random variable and the theory described in Section 1.2.1 is applied. The condition in Equations 1 and 2 is now augmented to include the value of the informative random variable, in addition to the action $\mathcal{A}$. This gives the expected value for the decision, conditioned on the value of the informative random variable. For the discrete case this is:

$$E\left[U|X=x,\mathcal{A}\right]=\sum_{i=1}^{n}P(\Omega=\omega_i\mid X=x,\mathcal{A})u(\omega_i), \tag{9}$$

To obtain the expected value regardless of the value of $X$, it is necessary to find the expectation of this expression with respect to $X$. However in doing so, it must be considered that the action taken can depend on the value of $X$, since this is known to the decision-maker. Suppose that some fixed decision policy, $D(x)$, is used to choose the action to take. Then the expected value that is obtained is:

$$E\left[U\right]=\sum_{x}P(X=x)E\left[U|X=x,D(x)\right]. \tag{10}$$

A decision policy that gives the greatest value for this expectation will be referred to as an optimal decision policy or *best policy*, and will be denoted by $D^*(x)$. The corresponding expected value will be denoted by $E^*[U]$. The difference between the expected value for an optimal policy when the value of the random variable $X$ is known to the decision-maker and that when the value of $X$ is unavailable will be referred to as the *significance* of the information and will be denoted by $\mathcal{S}(X)$. If the value of the information in terms of its significance does not exceed the cost of replacing it, then a nett loss would be incurred by replacing the information.

Standard Information Theory is sometimes criticised on the basis that all possible messages are considered to be equal and that, therefore, the theory does not reflect the humanistic notion of information. See, for example, references [1, ch. 4] and [17, ch. 2]. This objection can be overcome by associating a significance with each possible message or informative random variable value, as was done above. Then the value, $\mathcal{V}(X)$ of an information source $X$ can be quantified, in terms of utility units per bit, as the ratio of the significance of the informative random variable, $\mathcal{S}(X)$, to the mutual information, $\mathcal{I}(X,Y)$, between it and the situational random variable to which it applies:

$$\mathcal{V}(X)=\mathcal{S}(X)/\mathcal{I}(X,Y). \tag{11}$$

Of course, this value will be dependent on the utility units that are used and care should be taken only to compare values that are expressed in the same utility units.

Another way in which an information item may be valued is in terms of its *importance.* The importance of an information item is judged by its *potential* to improve decision-making, again applying the theory of Section 1.2.1. Thus, importance relates to how desirable it would be to achieve a better knowledge of an information item. Information importance is measured by the Expected Value of Perfect Information (EVPI), defined as the expected additional utility that could be achieved by an optimal decision policy if the item of information in question were known with certainty. A high value of EVPI for some information item would provide an indication to examine how well the information is presently known, and whether knowledge of it may be advantageously improved to enhance decision-making. On the other hand, an adversary in an Information Operations context might employ EVPI as a guide to targeting information to deny.

As discussed in Section 1.2.2, Information Theory shows that a signal must be sufficiently redundant to contain a certain amount of self-corroborating evidence in order to enable errors to be avoided, otherwise the message, which in this case might be a situation assessment report, that reaches the commander will contain errors with a probability approaching unity. A demonstration of this effect is the school-yard game of *Chinese Whispers* where a cascade of errors leads to the message that is eventually received bearing no resemblance to the original message. Such errors will tend to have a negative impact on utility because they will mislead the commander. Consequently, the corrupt information may be worse than valueless, and we must consider the possibility that information has a negative significance.

Therefore, a possible problem with using EVPI for targeting is that, although the EVPI for some item of information may be high, the actual information may in fact be so corrupt as to have negative significance. Targeting such information would be counterproductive. These considerations also raise the speculative possibility that in an information attack, in some circumstances, e.g., where there are long chains of command, it may be more effective to deny the corroborating part of the signal, rather than the entire signal, and rely on the resulting corruption of information to lead to the adversary taking actions that are disadvantageous to himself.

The value scales that are used for the valuation of significance and importance may be *objective* or *subjective.* Objective values are independent of the particular decision-maker being considered, whereas subjective values are dependent on the decision-maker concerned. While objective valuations are to be desired, it is sometimes only possible to assign a subjective value to information. Section 2.7 concerns an example of such a situation. Some mechanism may be required to achieve reasonable compromise values when diverging subjective valuations are arrived at by commanders with overlapping areas of responsibility.

### 1.2.4 Modelling Temporal Effects

In the work described by the present report, temporal modelling has been implemented using a form of Petri Net. A Petri Net is a formal notation for studying the behaviour of concurrent systems. We consider that two events occur concurrently if it is not possible to say whether one occurred before or after the other. A concurrent system is one in which concurrent events may arise. Petri Nets are useful in analysing the case where there are

interactions between events that restrict their concurrent occurrence and which therefore enable something to be deduced about the order in which they can occur. This enables some important properties of the system represented by the Petri Net to be deduced.

The "smallest", or atomic event, that can occur in a Petri Net is the "firing" of a single *transition*. Restrictions are placed on the firing of transitions through associating *input places* with them. A transition may only fire if certain conditions regarding the arrangement of tokens in input places are satisfied. When a transition fires, the *participating tokens*, i.e., those which cause the firing condition to be satisfied, are consumed and additional tokens may be generated in the input places of the transitions. The input places in which additional tokens may be generated as the result of a transition firing are known as the *output places* of the transition.

A Petri Net is represented as a bipartite graph, with the places (depicted as unfilled circles) forming one set of nodes and the transitions (depicted as lines or rectangles) the other. Arcs (directed links) connect input places to their corresponding transitions and transitions to their output places. To specify a Petri Net it is necessary to specify both its graph $G(P \cup T, A)$ and an *initial marking* $M_\emptyset$ of the places in the graph. This marking indicates which places initially contain tokens.

Traditional Petri Nets contain only tokens of the one type and the rules which enable the firing of transitions are simple. The conciseness of Petri Net models can be greatly enhanced by allowing tokens of different types, where each type may have a number of properties associated with it. Such Petri Nets are termed "coloured" Petri Nets because the different token types can be imagined as tokens of various colours, whereas traditional Petri Nets, conceptually, contain only black tokens. An alternative term used to describe these is "high-level" Petri nets. As a result of this diversity, the firing rules become more elaborate and need to be explicitly stated by the analyst. This is usually done using some formal computer language or mathematical logic.

Another useful extension is to include time in the Petri model. This can be done in various ways. For example, it may be considered that some period time must elapse after a condition becomes satisfied before a transition enabled by that condition may fire. Alternatively, it may be considered that a token can only participate in the firing of a transition after it has existed in a place for a certain period of time. Petri nets which include such timings are termed timed Petri nets. Timed Petri nets can be further generalised to include the case where times are governed by stochastic processes, to yield stochastic Petri nets. The term stochastic Petri net is normally only used for the case where the transition is timed. However, in this report it will also be considered to include the case of stochastically-timed places.

With extensions such as those described above, coloured Petri nets become a potent general purpose simulation tool, but with the advantage that certain fundamental properties of the model can be analysed using the techniques of Petri Net theory.

The transient and steady-state behaviours of stochastic Petri nets can be analysed using queueing network theory. The places in the Petri net correspond to queues in a related queueing network, and the firing of transitions in the Petri net correspond to the servicing of customers in the queueing network.

In order to organise complex Petri nets in manner that can be readily interpreted by

a human analyst, a hierarchical system can be introduced, where places and transitions in net higher in the hierarchy correspond to complete subnets at a lower level in the hierarchy. This principle can be taken still further by employing the concepts of object-oriented system design. A number of software packages are available which implement a variety of Petri net formalisms. This makes the use of Petri nets a convenient analysis tool for a wide range of problems. In Section 3 we demonstrate how Petri Nets may be applied to modelling a decision-making organisation. Some other examples of the application of coloured Petri nets to modelling military decision making organisations are given by Levis [5], Perdu [11] and Ray [13].

# 2 Secular Analysis

This section will first describe a simple example of a decision problem faced by a commander. It will then proceed to demonstrate how the problem may be analysed by applying the concepts explored in Sections 1.2.1 through 1.2.3. Information Theory, which was described in Section 1.2.2, will be applied in Section 2.2 to calculate the quantity of information reaching the commander. The two decision-theoretic techniques mentioned in Section 1.2.1 will be demonstrated and compared.

The first technique will be to employ a conventional Decision Tree and this is described in Section 2.4. The second technique will represent the problem in the form of an Influence Diagram. This is described in Section 2.5. Before these techniques can be applied, however, it will first be necessary to determine an appropriate utility scale. This is done in Section 2.3. The commander's best policy is then given, which can be determined either directly from the Decision Tree or from the Influence Diagram, using an appropriate software tool.

Section 2.7 will use decision-theoretic techniques to calculate the quality of the information reaching the commander in terms of its significance and its importance. It will also calculate the value of the information reaching the commander from its significance and quantity. Section 2.8 will examine the effects that Information Warfare could have on the results of the analysis. These effects are quantified numerically.

The term *secular analysis* has been chosen for this part of the analysis because temporal relationships are not yet considered at this stage. Section 3 considers how temporal effects may be subsequently included.

## 2.1 Scenario

The following simple scenario will be considered. A commander must decide whether to engage an enemy contingent. To assist him in this task, he uses his troops to reconnoitre the enemy and so obtain intelligence on its strength. Of course, the enemy may attempt to defeat such activities by taking efforts to conceal the true strength of its forces and thereby achieve an element of surprise. Once the commander has an estimate of the strength of the enemy he must decide whether to attack or leave the enemy force unchallenged. It he decides to attack, the outcome, either victory or defeat, of the combat depends

| Enemy Strength | |
|---|---|
| Strong | Weak |
| 0.7 | 0.3 |

*Table 1: Enemy Strength Distribution*

| Enemy Strength | Intelligence | | |
|---|---|---|---|
| | Strong | Unknown | Weak |
| Strong | 0.7 | 0.2 | 0.1 |
| Weak | 0.15 | 0.25 | 0.6 |

*Table 2: Intelligence Conditional Distribution*

stochastically on the true enemy strength. This example will be used to explore the application of various analytical techniques to Information Operations.

It is assumed that the intelligence gathered takes one of the three forms "Enemy Strong", "Enemy Strength Uncertain" and "Enemy Weak". It is necessary to assume a prior distribution for enemy strength, and a conditional distribution for the intelligence reported for each level of enemy strength. The combat effectiveness of the troops is also required. This will be specified as a conditional probability distribution which gives the probability of victory and defeat conditioned on the strength of the opposing force.

These should come from the commander's knowledge of his enemy and his intelligence processes, as well as his past experience. The challenge in applying the techniques described here will be to achieve reasonable choices for the distributions based on the available information and experience. It will be a matter for additional research to determine how this can best be achieved. For the present, it is merely assumed that it is possible to elicit the required values.

The enemy strength distribution is given in Table 1 while the intelligence conditional distribution is given in Table 2. The assumed combat effectiveness of the troops is given in Table 3.

## 2.2 Intelligence Information Quantity

This section applies the theory of Section 1.2.2 to the scenario given in Section 2.1. The "channel" for this case is shown in Figure 2.

| | Enemy Strength | |
|---|---|---|
| Outcome | Strong | Weak |
| Defeat | 0.9 | 0.1 |
| Victory | 0.1 | 0.9 |

*Table 3: Troop Combat Effectiveness*

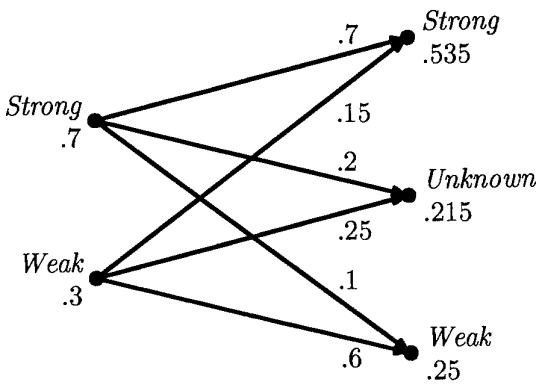



*Figure 2: Intelligence Channel*

The *marginal entropy* of the *Enemy Strength* random variable $S$ is given by

$$\begin{aligned} \mathcal{H}(S) &= -\sum_s \log_2 P(S=s) \cdot P(S=s) \\ &= -.7 \times \log_2(.7) - .3 \times \log_2(.3) \\ &= 0.88. \end{aligned} \tag{12}$$

The marginal entropy $\mathcal{H}(S)$ provides an indication of the amount of uncertainty that exists concerning the *Enemy Strength* random variable when no intelligence information is available. Since logarithms to the base of 2 are used, the resulting figure is in units of binary digits (bits) or Hartleys. For two equi-probable outcomes, the entropy would be 1.0. This is the maximum possible entropy for this random variable. The actual figure is less than the maximum because the probability of one of the values is *a priori* greater than that of the other. Therefore there is already some information concerning the likely value. If the value were known *a priori* with certainty, the entropy would be zero.

Similarly, the marginal entropy of the *Intelligence* random variable $I$ is given by

$$\begin{aligned} \mathcal{H}(I) &= -\sum_i \log_2 P(I=i) \cdot P(I=i) \\ &= -\sum_i \log_2 \left[\sum_s P(I=i|S=s)P(S=s)\right] \cdot \sum_s P(I=i|S=s)P(S=s) \\ &= -.535 \times \log_2(.535) - .215 \times \log_2(.215) - .25 \times \log_2(.25) \\ &= 1.46. \end{aligned} \tag{13}$$

Conversely to the previous case, $\mathcal{H}(I)$ provides an indication of the amount of uncertainty that exists concerning the *Intelligence* random variable when the value of the *Enemy Strength* random variable is unknown. This quantity is not of direct relevance to the present problem, but enters into some of the subsequent calculations below. The value is greater than 1.0, which was the greatest possible value in the previous case because there are now three possible values instead of only two as before.

The entropy of the random variables $I$ and $S$, considered jointly, is given by

$$\mathcal{H}(I,S) = -\sum_{i,s} \log_2 P(I=i, S=s) \cdot P(I=i, S=s)$$

$$
\begin{aligned}
&= -\sum_{i,s} \log_2 \left[P(I=i|S=s)P(S=s)\right] \cdot P(I=i|S=s)P(S=s) \\
&= -.49 \times \log_2(.49) - .14 \times \log_2(.14) - .07 \times \log_2(.07) \\
&\quad - .045 \times \log_2(.045) - .075 \times \log_2(.075) - .18 \times \log_2(.18) \\
&= 2.10 \qquad (14)
\end{aligned}
$$

This *joint entropy* indicates the amount of uncertainty that exists in a random variable consisting of an ordered pair formed from the *Intelligence* random variable and the corresponding *Enemy Strength* random variable. If these two random variables are independent, their joint entropy is simply the sum of their individual entropies. In fact the value of the joint entropy is $2.10 < 1.46 + 0.88 = 2.34$, demonstrating that the two random variables are interdependent. Again, this quantity is not of direct relevance to the present problem, except as an indication of the independence or otherwise of the random variables. It does, however, enter into subsequent calculations below. There are six possible values for the pair $(I, S)$. The maximum value of joint entropy occurs when these are equally likely. This maximum value is $\log_2 6 = 2.59$.

The *conditional entropy* of the random variable $S$, given that the value of the random variable $I$ is known, is given by

$$
\begin{aligned}
\mathcal{H}(S|I) &= -\sum_{s,i} \log_2 P(S=s|I=i) \cdot P(S=s, I=i) \\
&= -\sum_{s,i} \left[\log_2 P(S=s, I=i) - \log_2 P(I=i)\right] P(S=s, I=i) \\
&= \mathcal{H}(S,I) - \sum_{i} \log_2 P(I=i) \cdot \sum_{s} P(S=s, I=i) \\
&= \mathcal{H}(S,I) - \mathcal{H}(I) \\
&= 2.10 - 1.46 \\
&= 0.64 \qquad (15)
\end{aligned}
$$

This may be interpreted as the amount of uncertainty that remains regarding the value of the *Enemy Strength* random variable when the value of the *Intelligence* random variable is known. It can be seen that its value must be less than the joint entropy of the two random variables. It is included here because it is of direct relevance to the present problem. In fact, the quantity that is of greatest interest is the difference between the marginal entropy of the *Enemy Strength* random variable and this entropy. It was shown in Section 1.2.2 that it is possible to calculate this difference directly from the previously computed values without the necessity of computing the conditional entropy itself. This difference is simply equal to the mutual information of the two random variables. The value of the conditional entropy has only been computed here for interest.

The *mutual information* of $I$ and $S$ is given by

$$
\begin{aligned}
\mathcal{I}(I,S) &= \mathcal{H}(I) + \mathcal{H}(S) - \mathcal{H}(I,S) \\
&= 1.46 + 0.88 - 2.10 \\
&= 0.24. \qquad (16)
\end{aligned}
$$

As stated above, this value indicates the reduction in uncertainty in the value of the *Enemy Strength* random variable that a knowledge of the value of the *Intelligence* random variable

| Outcome | Satisfaction |
|---|---|
| Engagement with weak enemy contingent | 100 |
| No engagement with strong enemy contingent | 70 |
| No engagement with weak enemy contingent | 20 |
| Engagement with strong enemy contingent | 0 |

*Table 4: Utility Function*

provides. Because it is a symmetric measure, it also provides an indication of the converse, i.e., the reduction in uncertainty about the *Intelligence* random variable that a knowledge of the *Enemy Strength* random variable provides. It is zero if the two random variables are independent. From Equation 8, it must be less than than the minimum of the two marginal entropies of the random variables, since it is assumed that it is not possible to remove information by providing additional information and entropy is always positive. The mutual information is of such interest because it gives a measure of the *quantity of information* that a knowledge of the value of the *Intelligence* random variable provides about the value of the *Enemy Strength* random variable.

## 2.3 Utility Scale

A utility function provides a measure of the relative advantage (or conversely, disadvantage) of each possible outcome. The utility function used in this example (see Table 4) will be the abstract notion of the degree of satisfaction that each possible outcome gives the commander. Arbitrary values are assigned on a scale of 0 to 100 points or *utiles*. The commander will be most satisfied if the enemy is weak and an engagement takes place, since he then has the greatest chance of achieving victory. The next highest level of satisfaction occurs when the enemy is strong and no engagement is undertaken, since the commander then avoids the likelihood of defeat. If the enemy is weak and no engagement is undertaken, a good chance for victory is foregone, which is unsatisfactory. The least satisfactory outcome is that where engagement occurs and the enemy is found to be strong, since then the chance of incurring defeat is high.

The utility scale that has been chosen here is an arbitrary one. For example, 20 could be changed to 40 and 70 could be changed to 45 without affecting the preference ordering between the outcomes. The problem is how to determine such a scale in a practical manner so that the differences in the satisfaction values, i.e., the marginal utilities, have a useful meaning. This question is addressed by references [12, ch. 4] and [3, ch. 4], and can be answered by introducing the notion of lotteries. The resulting utility scales are, however, subjective ones.

As an example of how this procedure would be applied, a commander would need to ask himself what his preferences were with respect to, say, escaping engagement with a strong enemy, compared with a lottery where he had a chance $\alpha/100$ of engaging a weak enemy and a chance $(1-\alpha)/100$ of inadvertently engaging a strong enemy. The two alternatives in the lottery are the most favoured and least favoured outcomes. These are assigned utilities 100 and 0, respectively. The value $\alpha$ for which the commander is

indifferent between the two choices is the utility that is then associated with escaping engagement with a strong enemy. Associating a utility value of 70 with this outcome implies that the commander is indifferent to the choice of escaping engagement with a strong enemy, and a lottery where he has a probability of 0.7 engaging a weak enemy and probability of 0.3 of engaging a strong enemy.

## 2.4 Decision Tree

The Decision Tree, which corresponds to the scenario that is described in Section 2.1, is shown in Figure 3. The circular nodes in the Decision Tree represent discrete random variables. There is a branch out of these nodes for each possible value of the random variable. These branches are marked with the conditional probability that the value the represent occurs.

The square nodes represent discrete decision variables. There is a branch out of the node for each possible decision choice. These branches are marked with the conditional expected utility associated with the decision choice they represent. The right-most branches of the Decision Tree display the conditional expected utilities that result from each possible combination of circumstances and decision choice. In fact, these values are deterministic for this tree, since once the enemy strength is known with certainty, the values for the two decision alternatives are known definitely.

The problem to be solved is how to make the best decision when the enemy strength is not known for certain, but where there is only an intelligence report available, which is not completely reliable, on which to make a decision. To do this, a Decision Tree is needed from which the *Enemy Strength* random variable has been removed. This will be termed a folded tree because, conceptually, all the alternatives for the *Enemy Strength* random variable are folded together into one.

This is achieved by "marginalising" the *Enemy Strength* random variable. The mathematical details of this procedure are given in Appendix A. A folded version of the original tree in which the *Enemy Strength* random variable is marginalised away is shown in Figure 4. The details of the calculations involved are shown on the diagram. The optimal decision policy can be read directly from this tree. It is given later in Section 2.6, in Table 6.

## 2.5 Influence Diagram

An Influence Diagram representing the example problem is shown in Figure 5. The boxes with rounded end caps represent the random variables, which in this case are *Intelligence* and *Enemy Strength*. Rectangular boxes represent decision variables. In this case there is only one decision variable, corresponding to the commander's decision on whether to launch an attack on the enemy. The box with triangular end caps represents the utility random variable. There is only one of these in any Influence Diagram. In this case, it represents the commander's satisfaction.

The arrow from the *Enemy Strength* random variable box to the *Intelligence* random variable box indicates that the *Intelligence* random variable is conditionally independent

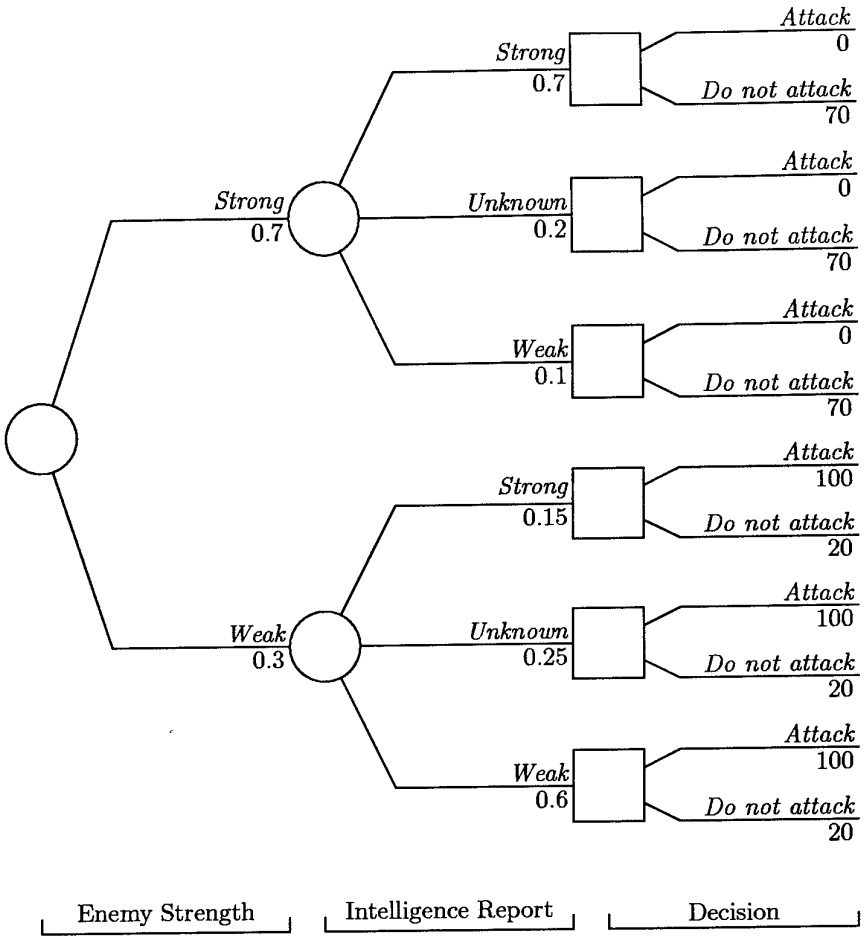



*Figure 3: Decision Tree*

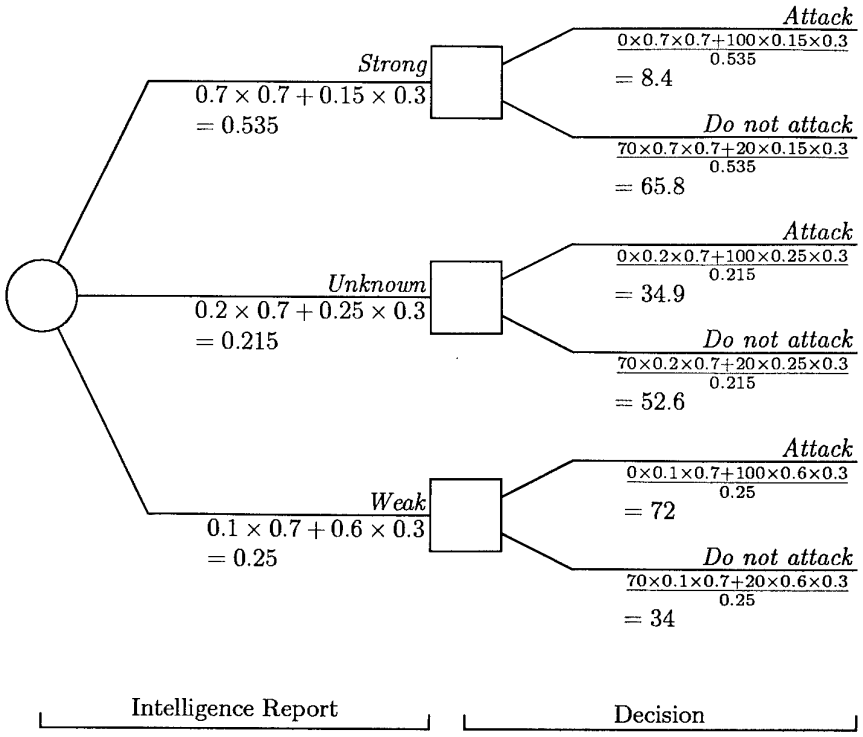



*Figure 4: Folded Decision Tree*

of all other random variables given the value of the *Enemy Strength* random variable. The arrow from the *Intelligence* random variable box to the *Launch Attack* decision variable box indicates that the decision that is made depends only on the value of the *Intelligence* random variable. The arrows from the *Enemy Strength* random variable box and the *Launch Attack* decision variable box indicate that the value of the *Commander's Satisfaction* utility random variable is conditionally independent of the value of the *Intelligence* random variable given the values of the *Launch Attack* decision variable and the *Enemy Strength* random variable. It can be seen that the Influence Diagram for the problem provides a more succinct graphical representation than does the Decision Tree.

A conditional probability table is associated with each of the random variable boxes in the Influence Diagram. The number of conditioning variables in the table is equal to the number of arrows leading into the random variable box. There is a row in the conditional probability table for each possible combination of the states of the conditioning random variables. The conditioning random variables are termed the *parents* of the random variable box. The number of columns in each of these rows is equal to the number of possible outcome values for the random variable. Each outcome is assigned a probability for every combination of conditioning random variable states. The conditional probability tables for the *Enemy Strength* and *Intelligence* random variables are just those given in Tables 1 and 2.

Similarly, a decision table is associated with each of the decision variable random boxes. This table gives the value of the decision variable for every combination of values of its parent variables. It therefore represents the decision policy of the decision-maker

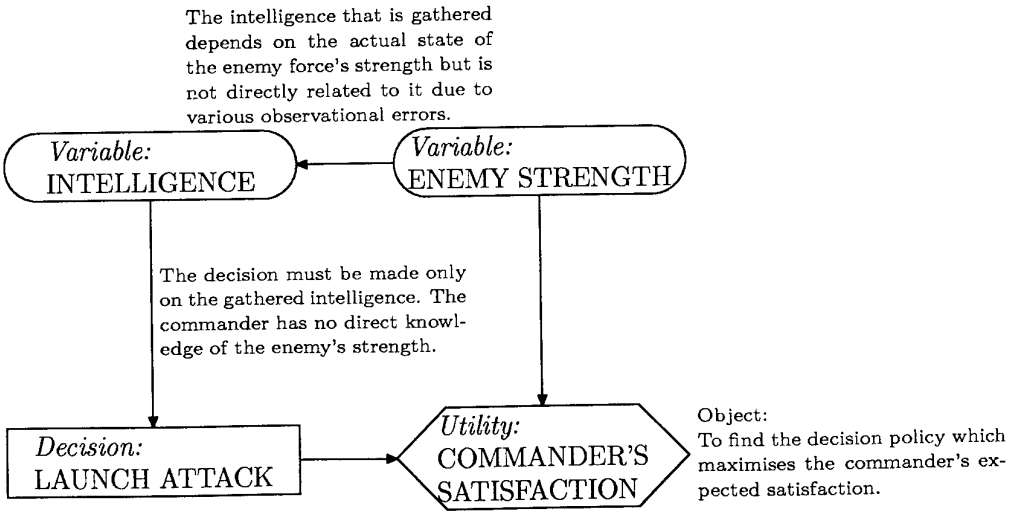



*Figure 5: Influence Diagram for the Command Example*

| Enemy Strength | Launch Attack | Satisfaction |
|---|---|---|
| Weak | NO | 20 |
| Weak | YES | 100 |
| Strong | NO | 70 |
| Strong | YES | 0 |

*Table 5: Conditional Utility*

and the solution to the decision problem. The best policies for the decision variables which maximise the expected value of the utility variable can be conveniently found from the Influence Diagram by using an automated software tool, such as that described in reference [9].

Finally the utility random variable box has associated with it a utility table which gives the utility value that is associated with every combination of values of its parent variables. This is shown in Table 5.

## 2.6 Best Policy

From the scenario details given in Section 2.1, the commander's best action for each intelligence outcome can be inferred, using utility theory as discussed in section 1. His best policy, as derived by this theory, is given in Table 6. This policy can be read from the Decision Tree in Figure 4 or can be computed from the Influence Diagram in Figure 5 using a BBN software package that also supports Influence Diagrams, such as that described in reference [9]. This software package supports Influence Diagrams as an extension of ordinary BBNs.

The probabilities for the engagement outcomes with this policy, the combat effective-

| Intelligence | Engage? |
|---|---|
| Enemy strong | NO |
| Enemy strength uncertain | NO |
| Enemy weak | YES |

*Table 6: Commander's Best Policy*

| | Engagement Outcome | | | |
|---|---|---|---|---|
| IW Option | None | Victory | Defeat | Victory\|Combat |
| None | 0.75 | 0.169 | 0.081 | 0.676 |
| Denial | 1.0 | 0.0 | 0.0 | - |
| Deception (Pretense) | 0.817 | 0.108 | 0.074 | 0.593 |
| Deception (Feint) | 0.54 | 0.19 | 0.27 | 0.413 |
| Psychological Operations | 1.0 | 0.0 | 0.0 | - |

*Table 7: Engagement Outcome Distribution for Best Policy*

ness specified in Table 3, and with no IO against the commander present are given in the first row of Table 7. Following sections will consider the effects that various IO produce. The outcome probabilities for these are also included in Table 7. These additional four rows should be ignored at this stage.

## 2.7 Intelligence Information Quality

Now, what can be said of the value of the intelligence to the commander? In the foregoing example, the commander's expected satisfaction for the optimal decision policy is $0.535 \times 65.8 + 0.215 \times 52.6 + 0.25 \times 72 = 64.5$ utiles, or units of satisfaction, where the values have been taken from the decision tree in Figure 4. This value can be compared with the case where no intelligence is available of $0.7 \times 70 + 0.3 \times 20 = 55.0$ utiles, where the appropriate values have been taken from Tables 1 and 4. This assumes that no attack is made when intelligence information on the situation is unavailable, which is the best policy in this situation. Taking the difference of these two values gives the *significance* of the intelligence information to the commander. Therefore, the significance of the intelligence to the commander is currently $\mathcal{S}(I) = 64.5 - 55.0 = 9.5$ utiles. It may also be of interest to establish what the value of improved intelligence might be to the commander. The upper limit on this value occurs when the intelligence is always correct. In that case the commander's satisfaction is found to be $0.7 \times 70 + 0.3 \times 100 = 79$ utiles, where the appropriate values have been taken from Tables 1 and 4 again. Therefore, the expected value of perfect information is $79 - 55 = 24$ utiles, which gives the *importance* of the intelligence information. The current intelligence information supplies less that half of the additional satisfaction that could be achieved through improved intelligence. Therefore improving intelligence is potentially worthwhile. The results also indicate that the commander is not particularly vulnerable to the destruction and denial aspects of IW in this case because the greatest decrease in satisfaction that could be achieved through this means would be 9.5 utiles out of a total of 64.5, or 14.7 per cent. However, he may

be more vulnerable to other forms of IW as described in Section 2.8.

These information values are subjective because the utility scale that is used represents the personal preferences of the commander. Different values might be obtained for different commanders. It is assumed that these differences would be slight for commanders from the same force, since they would have similar culture and training. However, they might be substantially different for commanders with differing cultural backgrounds and training, such as those of foreign forces, particularly potential adversary forces. This must be accounted for if the techniques described in this report are to be applied to analysing adversary decision-making organisations.

Finally, the value of the intelligence information, calculated as the ratio of its significance to its quantity, is $\mathcal{V}(I) = \mathcal{S}(I)/\mathcal{I}(I,S) = 9.5/0.24 = 39.6$ utiles per bit, where $\mathcal{I}(I,S)$ was calculated in Section 2.2. This can be compared with the case of perfect information, where $\mathcal{H}(S|I) = 0$ and hence $\mathcal{I}(I,S) = \mathcal{H}(S) - \mathcal{H}(S|I) = \mathcal{H}(S)$. In that case, the value of the intelligence information is $24/0.88 = 27.3$ utiles per bit, where the expected value of perfect information was calculated above and the value of $\mathcal{H}(S)$ was computed in Section 2.2. This demonstrates that a law of diminishing returns applies as the quantity of available information increases in this case.

## 2.8 Secular Effects of Information Warfare

This section examines those effects on the commander's decision process that IW actions may have that do not directly arise from temporal relationships. These fall into three general categories, which are information denial, deception and psychological operations. The deception category has been divided into two subcategories, deterring attack by pretending to have a greater strength than the actual strength, and seducing an adversary into attack by feigning a weaker strength than the actual strength. These effects have been termed secular effects because they do not explicitly relate to time. The warfighting disciplines which contribute to these effects include operational secrecy, emission control, signature reduction, electronic warfare, psychological operations as well as physical targeting of information related installations.

Effects that relate directly to time have been termed temporal effects. Examples of these are information delay and decision-making time prolongation. Discussion of these effects is deferred to Section 3.5.

### 2.8.1 Information Denial

In this example, denial of the availability of intelligence information to the commander is modelled by fixing the value of the *Intelligence* random variable to the value "Unknown". Since the best policy when the intelligence variable has this value is not to attack, if the adversary succeeds in denying intelligence information to the commander he will avoid being attacked, which is assumed to be his IW aim. As discussed in Section 2.7, the value of the information is 9.5, therefore this must also be the information value of an IW or concealment operation which denies the information to the commander.

| Enemy Strength | Intelligence | | |
|---|---|---|---|
| | Strong | Unknown | Weak |
| Strong | 0.7 | 0.2 | 0.1 |
| Weak | 0.375 | 0.25 | 0.375 |

*Table 8: Pretense Conditional Distribution*

If the adversary's aim is to lure the commander to attack a strong enemy contingent, this cannot be achieved through denial of information. The adversary must instead resort to deception as described in Section 2.8.2.

### 2.8.2 Deception

Deception may be regarded as an IO in that it may either entail falsification of information or selective denial of information, or a combination of both.

There are two possible cases of deception to consider in this example. If the enemy contingent strength is weak then the adversary's aim is to deceive the commander that it is strong to avoid attack. If the enemy contingent strength is strong the adversary might seek to lure the commander to attack by deceiving him into believing that the contingent strength is weak. The effects of deception would be included in the decision model presented above by using a different conditional probability distribution for calculating the outcomes from that used for calculating the commander's best policy. The disparity between the two indicates the degree of deception. The disparity will be quantified by the difference in the expected utilities produced by the two distributions when the best policy, as deduced from the original distribution, is applied.

First consider the case where the object is to deceive the commander by pretending that a weak enemy contingent is strong. Suppose that this pretense results in the conditional probabilities for the intelligence information shown in Table 8. The values in this table assume that the pretense is successful to the extent that a weak enemy contingent is as likely to be reported as strong as it is to be reported weak. The probability that the strength of a weak enemy cannot be determined has not been changed. The probabilities associated with a strong enemy contingent also remain the same. For this conditional probability distribution, and for the best policy determined earlier, the expected utility is 59.1 utiles. Therefore, in information terms, the value of the deception operation has been $64.5 - 59.1 = 5.4$ utiles.

Now consider the case where the enemy contingent is strong and the object is to deceive the commander by feigning that it is weak in order to lure him into combat. Suppose that the conditional probability values for the intelligence information shown in Table 9 are the result of such a feint. The values assume that the feint is successful to the extent that a strong enemy contingent is equally likely to be reported weak as to be reported strong. The probability that the strength of a strong enemy cannot be determined has not been changed. The probabilities associated with a weak enemy contingent also remain the same. For this conditional probability distribution, and for the best policy determined earlier, the expected utility is 49.8 utiles. Therefore, in information terms, the value of

| Enemy Strength | Intelligence | | |
|---|---|---|---|
| | Strong | Unknown | Weak |
| Strong | 0.4 | 0.2 | 0.4 |
| Weak | 0.15 | 0.25 | 0.6 |

*Table 9: Feint Conditional Distribution*

| Outcome | Satisfaction |
|---|---|
| Engagement with weak enemy contingent | 58.9 |
| No engagement with strong enemy contingent | 100 |
| No engagement with weak enemy contingent | 20 |
| Engagement with strong enemy contingent | 0 |

*Table 10: Overcautious Utility Function*

the deception operation would be $64.5 - 49.8 = 14.7$ utiles.

It is evident from the above that feigning weakness, with an information value of 14.7 utiles would be a more effective deception operation than would be pretending strength with an information value of 5.4 utiles.

### 2.8.3 Psychological Operations

The commander's subjective utility scale affects his choice of best policy. For the subjective utility values shown in Table 10, he is indifferent to attacking when intelligence indicates the enemy is weak, whereas, for the original scale defined in Table 4, he would attack in this case. This utility scale borders on the case of an overly cautious attitude, where no attack will be made on the enemy no matter what the intelligence on the enemy strength is.

On the other hand, for the utility values shown in Table 11, he would be equally inclined to attack as not to do so when an intelligence estimate of the enemy strength was not available, indicating a less cautious attitude than the original one. The engagement outcome probabilities for this policy are given in Table 12.

Thus it has been shown that it is possible to reflect different attitudes on the part of the commander by choosing different utility scales even when the scale is abstract. This enables the effect of psychological operations to be included in the decision model

| Outcome | Satisfaction |
|---|---|
| Engagement with weak enemy contingent | 100 |
| No engagement with strong enemy contingent | 42.8 |
| No engagement with weak enemy contingent | 20 |
| Engagement with strong enemy contingent | 0 |

*Table 11: Incautious Utility Function*

| IW Option | Engagement Outcome | | | |
|---|---|---|---|---|
| | None | Victory | Defeat | Victory\|Combat |
| None | 0.535 | 0.25 | 0.215 | 0.538 |
| Denial | 0.0 | 0.34 | 0.66 | 0.34 |
| Deception (Pretense) | 0.602 | 0.188 | 0.208 | 0.475 |
| Deception (Feint) | 0.325 | 0.272 | 0.404 | 0.402 |
| Psychological operations | 0.75 | 0.169 | 0.081 | 0.676 |

*Table 12: Engagement Outcome Distribution for Incautious Policy*

presented above by appropriately modifying the commander's subjective utility scale. For example, it would be expected that adversary psychological operations would tend to have the effect of rendering the commander more cautious.

Suppose that adversary psychological operations were effective to the extent that the commander's subjective utility function was modified to that in Table 10, and that, consequently, he avoids engaging the enemy in all cases. The value of the psychological operations in information terms can be determined by calculating the expected subjective utility for this new policy using the original, unaffected utility function and subtracting the value for the original policy. The original expected utility for the new policy is 55.0 utiles. Hence the information value of the psychological operations would be $64.5 - 55.0 = 9.5$ utiles, the same as it was for the case when information was denied.

The change in the commander's attitude movement, or *swing*, can be measured by the difference in expected utility obtained from the two utility functions when the new policy is adopted. The new expected utility for the new policy is 76.0, so his attitude movement comprises a swing of $76.0 - 55.0 = 21.0$ utiles towards the new policy. The swing provides a measure of the effectiveness of IO which might be useful for IW "Battle Damage Assessment".

## 2.9 Summary

Influence Diagrams are a relatively recently developed technique for representing decision-theoretic problems. They should be used in preference to the more traditional decision tree representation of such problems because of their ability to represent the problem in a general form without specifying in advance what are unknowns and what are givens. Automated tools allow the solution of a specific instance of the problem to be obtained directly from the Influence Diagram. Where such a tool is not available, a decision tree for a particular instance of the problem can be manually developed from the Influence Diagram and used to compute a solution. Adopting this two stage procedure allows some common errors that occur in constructing decision trees to be avoided.

This section has demonstrated how Influence Diagram methods may be used to reduce the problem of placing a subjective value on an item of information to one of estimating a conditional probability distribution and of determining a subjective utility function. It also has shown how similar techniques can be applied to evaluating several types of IO.

| IW Option | Value [Utiles] |
|---|---|
| Denial | 9.5 |
| Deception (Pretense) | 5.4 |
| Deception (Feint) | 14.7 |
| Psychological Operations | 9.5 |

*Table 13: Effectiveness of IW Options*

Although the application of Influence Diagrams has not completely solved the problem in its entirety, it has decomposed it in a useful way which allows more readily grasped analytical insights to be applied. In the next section a Coloured Petri Net model of the problem will be employed to allow various time related performance statistics to be obtained when the optimal decision policy derived from the Influence Diagram is applied. Such a temporal model also allows time related effects to be studied, which a static Influence Diagram model on its own does not.

It has also shown how it is possible to compare the effectiveness of IW options, from the point of the commander, by evaluating their effectiveness in terms of subjective utility. These evaluations are also relevant from the adversary's point of view if it is assumed that the commander and his adversary share similar subjective utility functions, and that the commander's loss is his adversary's gain, that is, that the situation is a zero-sum game, as described by von Neumann [16, ch. 3]. As remarked earlier, the assumption that protagonist and adversary share similar subjective utility functions needs to be treated with caution. Table 13 summarises the utility values that were obtained for the four IW options that were considered above.

It can be seen that the most effective option for this example is deception by feigning weakness and luring the commander's troops to likely defeat. Information denial and psychological operations can be equally effective by paralysing the commander into inaction. The least effective option is deception by pretending strength when it is only partially successful. In practice, a sensitivity analysis should be performed to determine how these conclusions are affected by uncertainties in the probability distribution parameters

Finally, it has been shown how the movement in a commander's attitude as the result of psychological operations, which has been termed "swing" can be measured on the same utility scale.

# 3 Temporal Analysis

The secular analysis presented in Section 2 demonstrated an approach based Influence Diagram methodology that can be used to determine optimal decision policies under uncertainty. However, that analysis ignored time-dependent effects. A temporal model, which is what is required to be able to analyse such effects, is described in this section. It uses a methodology which is based on hierarchical Coloured Petri Nets (CPNs). The scenario employed in this section is similar to the original one used Section 2, however it contains some additional details that were not relevant to the secular analysis performed

there. In particular, additional actors, besides the commander, are introduced. The term "actor" is used here to mean some discrete element of the model which can be considered to act of its own volition. These actors represent human beings, human organisations or nature.

The CPN which for the elaborated model is described and performance statistics that are obtained from executing the model are discussed. In executing the model, It is assumed that the optimum decision policy determined earlier in Section 2.6 is adopted by the commander. The results obtained are also compared with those derived by applying queueing network analysis to the CPN, again assuming that the optimal policy is adopted.

## 3.1 More Detailed Scenario

In the scenario presented in this section, there are five actors, an *intelligence organisation*, which provides information to a *commander*, who has command of a body of *troops*, who face an *enemy*, who inserts troops into the commander's region of operations at irregular intervals. The final actor is *fate* which determines the outcome of encounters between the commander's troops and those of the enemy.

## 3.2 Model Design

The scenario model comprises a master CPN and several subordinate CPNs. The master CPN shows the way in which the subordinate CPNs at one level below in the hierarchy interact. In the form of Petri net used in this report, these subordinate CPNs correspond to *transitions* in the master CPN. An object-oriented methodology has been employed in which each transition is considered to be an instance of a transition class. The definition of that class specifies the subordinate CPN that is represented by the transition. This makes it simple to create models for situations in which there are several occurrences of elements sharing the same behaviour. In the present simple example, it has not been necessary to exploit this feature, since there is only one occurrence of each behavioural element.

The transitions interact through a number of master CPN places. These places are considered to be connected to transitions contained within the subordinate CPNs. The conditions under which tokens in the master CPN will be produced or consumed are determined by the details of the subordinate CPNs, which in turn are determined by the classes to which they belong.

The modelling methodology allows multiple levels of hierarchy. Thus, the subordinate CPNs may themselves also contain further subordinate CPNs. Again, it has not been necessary to exploit this feature in the present, very simple example.

In the descriptions of CPNs given in the following sections, the transitions described earlier are given preference over the transitions that are described later for the purpose of resolving conflicts between them.

### 3.2.1 Master Coloured Petri Net

The master CPN creates instances of several transition classes which encapsulate the behaviours of the actors in the model. The master CPN places hold tokens which represent the actors themselves, as well as various auxiliary entities such as intelligence reports, situation reports, commander's orders and combat outcomes.

Subordinate CPNs are used to define the behaviour of each transition class. The transition classes are *ENEMY*, *INTELO*, *COMMANDER*, *TROOP* and *FATE*. These encapsulate the behaviours of the actors to which they correspond. In this simple example, the transitions themselves can be referred to by the same identifiers because there is only one instance of each class. Otherwise, the transitions would need to be distinguished, for example by appending sequential integers to the class identifiers.

#### Description

The master CPN is depicted in Figure 6 which shows the connections between the transitions corresponding to the five actors above. Intelligence is communicated to the commander through intelligence reports, which occupy the place $I$. These are generated when the transition *INTELO* fires and the precondition for this to occur is that a new enemy troop must have entered the commander's region of operations.

The commander analyses these intelligence reports and issues orders to his troops which occupy the place $O$. Orders are generated when the *COMMANDER* transition fires and can be of two types (i.e., tokens of two different "colours") which are listed below.

- An order to reconnoitre the enemy troops in an attempt to determine the enemy's strength. In this case the precondition is the presence of an intelligence report token in the place $I$, since the commander must first know the approximate location of the enemy troops.
- An order to attack the enemy troops. In this case the precondition is that there be a reconnaissance report token in the place $R$ because the commander must first obtain a report on the strength of the enemy troops before he can apply the optimal decision policy.

Troops execute the orders issued by the commander. The presence of a troop token in the place $T_0$ indicates the physical availability of troops. The presence of a troop token in place $T_2$ indicates that that troop is engaged in combat with an enemy force. In the present example, there is only one troop token. If there were more than one, they would be labelled to allow them to be distinguished.

The precondition for the firing of the *TROOP* transition is the presence of commander's order, troop and enemy force contingent tokens in the places $O$, $T_0$ and $E$. The double arrows in Figure 6 indicate that the corresponding token may be immediately regenerated upon the firing of the transition. If the commander's order is of the reconnaissance type, a reconnaissance report token is generated in the place $R$ by the firing of the transition and troop token in place $T_0$ is regenerated, when the task is complete. Otherwise, when

| | |
|---|---|
| $E$ | Enemy troops |
| $I$ | Intelligence reports |
| $O$ | Commander's orders |
| $T_0$ | Own troops (standby) |
| $T_2$ | Own troops (engaged) |
| $R$ | Troops' reconnaissance reports |
| $\Omega$ | Outcomes of combat |

*Table 14: Significance of Master CPN Places*

the order is of the attack type, the troop token in place $T_0$ is consumed, and another is generated in the place $T_2$, indicating engagement with the enemy force. The *order* token is consumed by the firing of the transition.

Fate decides the outcome of engagements between the commander's troops and those of the enemy, based upon their relative strengths and on chance. The precondition for the firing of the *FATE* transition is the presence of a troop token in the place $T_2$, the presence of a corresponding enemy force contingent token in the place $E$ and a random time has elapsed since the token in place $T_2$ appeared. The random delay time is drawn from a negative exponential distribution with a mean value of $\tau_{T_2} = 2.0$ ticks. An outcome token, which may represent either "victory" or "defeat", is generated as a result of this transition firing. The troop token in place $T_2$ is consumed and one generated in place $T_0$ instead, to indicate the renewed availability of the troop. This simple model neglects the effects of attrition. It assumes that the troop can always be reconstituted, even after defeat.

The enemy enters the commander's region of interest at irregular intervals and if engaged and defeated in combat is annihilated. The *ENEMY* transition may fire if a token of type "victory" is present at the place $\Omega$ and a corresponding enemy force contingent token is present at place $E$. In this case the enemy force contingent token is consumed, indicating that the enemy force has successfully passed through the region. Enemy force contingent tokens that are reported as "strong" are also consumed because they are allowed to pass through the region without being engaged. The *ENEMY* transition fires irregularly without any precondition being satisfied thereby spontaneously generating new enemy force contingent tokens.

### Token Structure

This section describes the structure of the tokens found in the places appearing in the master CPN. The tokens appearing in place $E$ contain an indication of the strength of the enemy contingent as well as provision to retain the unique designation assigned by the intelligence organisation. This artifice allows correct matching of enemy force contingent tokens with other tokens as required. Enemy force contingent tokens that have not been processed by the intelligence organisation can be recognised as such by the fact that they have not had a unique designation assigned. The tokens appearing in place $I$ contain the unique designation of the enemy contingent to which they apply.

Tokens appearing in place $O$ contain an indication of the kind of order they represent,

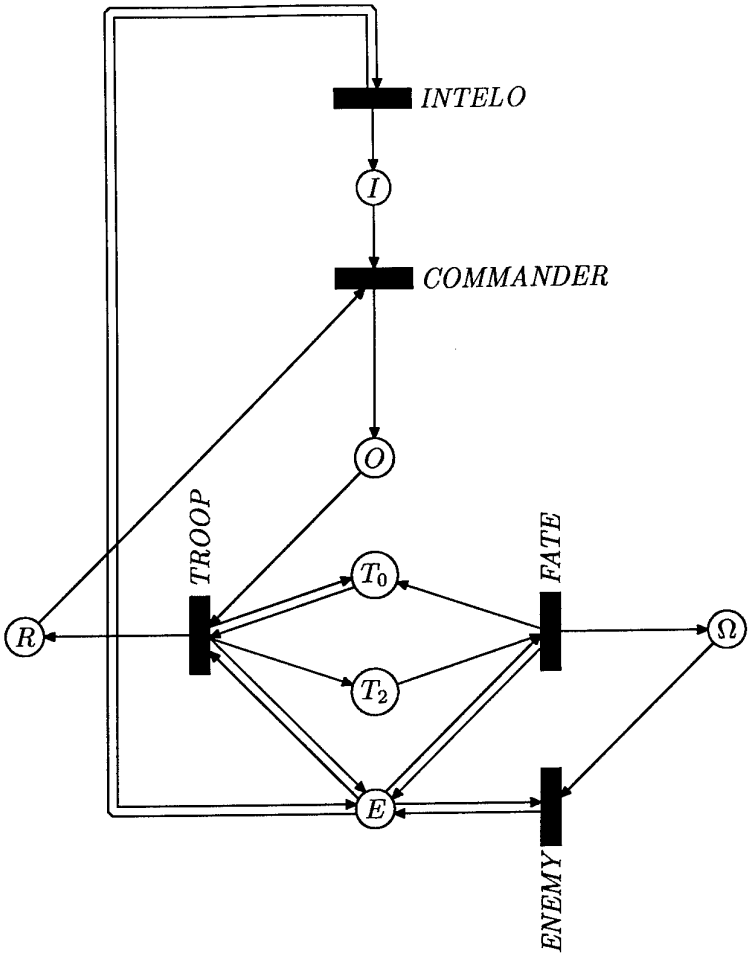



*Figure 6: Master CPN for the Command Example.*

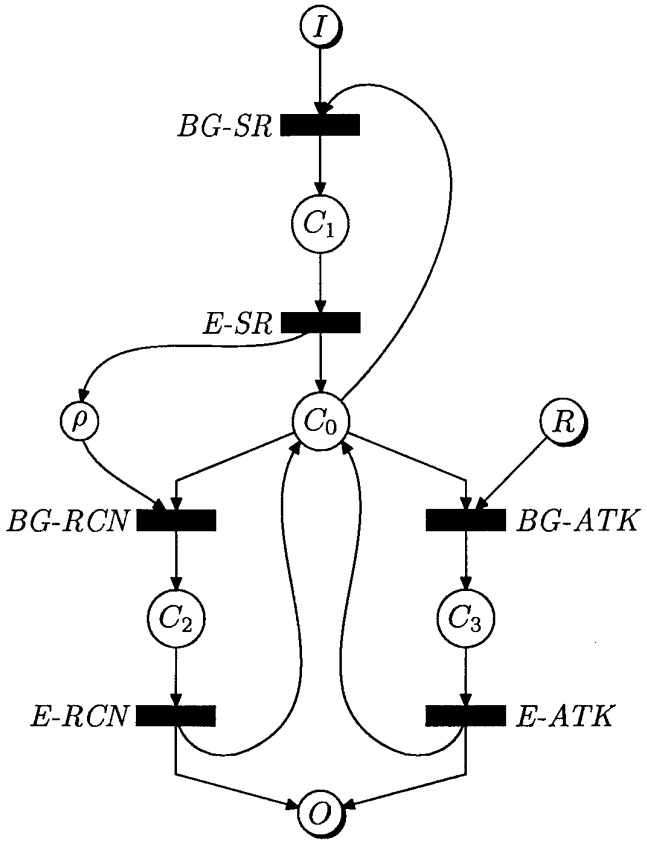



*Figure 7: Subordinate CPN for the "Commander" Component of the Command Example.*

as well as an indication of the enemy contingent to which they apply. Tokens appearing in place $R$ contain an indication of the enemy contingent to which they apply and an estimate of its strength, as assessed by the troop from a reconnaissance mission. Tokens appearing in places $T_0$ and $T_2$ contain an indication of the enemy contingent with which the troop is currently occupied. This indication will always be *null* for tokens in place $T_0$, which corresponds to the stand-by state. Tokens appearing in place $\Omega$ contain an indication of enemy contingent that was engaged in combat and an indication of what the outcome of that engagement was.

### 3.2.2 Commander Component

#### Description

The CPN for the commander actor is shown in Figure 7. The commander is assumed to be in one of four states at any one time, with each state being represented by its own place. It is necessary to use separate places for the states because, in the form of CPN used here, the timing aspects of the model are incorporated into the places. The places for the commander CPN are listed in Table 15 together with the symbols used to represent them. In addition to the command state places, there is a place $\rho$ which contains tokens

| | |
|---|---|
| $C_0$ | Commander not occupied with an identified task |
| $C_1$ | Digest situation report from intelligence organisation |
| $C_2$ | Formulate order for troop to conduct reconnaissance |
| $C_3$ | Formulate order for troop to engage enemy |
| $\rho$ | Recognition of new enemy troop entering region |

*Table 15: Significance of the* commander *CPN Places*

| | |
|---|---|
| *BG-SR* | Commander commences analysis of situation report |
| *E-SR* | Commander recognises that a new enemy troop has entered his region of operations |
| *BG-RCN* | Start formulation of order for troop to conduct reconnaissance |
| *E-RCN* | Issue order to troop to conduct reconnaissance |
| *BG-ATK* | Start formulation of order for troop to engage an enemy troop |
| *E-ATK* | Issue order to troop to engage an enemy troop |

*Table 16: Significance of the* commander *CPN Transitions*

indicating that particular enemy troops have been recognised as being in the region of operations by the commander.

The remaining places belong to the master net and have been passed to the subordinate net instance as parameters. Such places have been drawn with shadows on the diagrams and their meaning has already been explained in the discussion of the master diagram and in Table 14.

### Token Structure

The structure of the tokens that appear in the places $C_i$, $i = 0 \ldots 3$ includes an indication of with which, if any, enemy contingent the commander is currently dealing. This identity is obtained from the report tokens received from the subordinate CPN representing the intelligence organisation. The tokens appearing the the place $\rho$ have a similar structure.

### Transition Behaviour

For each of the places corresponding to the command states there are two transitions, one corresponding to the commander entering the state and the other to the commander leaving that state. The precondition for the *BG-SR* transition to fire is that the commander be currently idle and that a new situation report be available from the intelligence organisation. When the transition fires, the tokens in the places $C_0$ and $I$ are consumed, and a new token generated in the place $C_1$. Note that throughout the transition specifications in this report the identifier "enemy" is used to mean the designation of an enemy troop

contingent. Also, the symbol "=" is used to signify a condition of equality, while ":=" is used to signify an assignment operation.

*BG-SR:*

$\leftarrow C_0$

$\leftarrow I$

$\rightarrow C_1$ : enemy := enemy of token in input place $I$

The precondition for the *E-SR* transition to fire is that the commander token occupies place $C_1$ and a random delay has elapsed. The random delay time is drawn from a negative exponential distribution with a mean value of $\tau_{C_1} = 1.0$ tick. When the transition fires, the token in the place $C_1$ is consumed and is replaced with tokens in the places $C_0$ and $\rho$.

*E-SR:*

$\leftarrow C_1$

$\rightarrow C_0$

$\rightarrow \rho$ : enemy := enemy of token in input place $C_1$

The *BG-RCN* transition may fire when tokens are present in the $\rho$ and $C_0$ places, indicating that the commander is not otherwise occupied and that the presence of a new enemy troop in the region of operations has been recognised by the commander. The commander then enters the phase of preparing reconnaissance orders, which is represented by the token in the $C_0$ place being consumed and one being generated in the $C_2$ place. The appropriate token in the $\rho$ place is also consumed. Note that the $\rho$-tokens are marked with the identification code that the intelligence organisation has assigned to the enemy troop in question. This information is used to determine which enemy troop the reconnaissance order applies to.

*BG-RCN:*

$\leftarrow C_0$

$\leftarrow \rho$

$\rightarrow C_2$ : enemy := enemy of token in input place $\rho$

The *E-RCN* transition fires when there is a token present in the $C_2$ place and a random amount of simulated time has elapsed. The random time delay is drawn from a negative exponential distribution with a mean $\tau_{C_2} = 0.5$ ticks. Firing of the transition results in the token in the $C_2$ place being consumed and in tokens being generated in the $C_0$ and $O$ places. The token in the $O$ place has the reconnaissance order type. Tokens of order type are marked with the identifier of the enemy force to which they pertain so that they can be matched to the appropriate enemy force contingent token later.

*E-RCN:*

$\leftarrow C_2$

$\rightarrow C_0$

$\rightarrow O$ : kind := *recon*, enemy := enemy of token in input place $C_2$

The *BG-ATK* transition may fire when there is a commander token in place $C_0$ (i.e., commander is idle) and there is a reconnaissance report token in place $R$. When the *BG-ATK* transition fires the two input tokens are consumed and commander token is generated in the $C_3$ which represents the state where the commander is preparing orders for troops to engage an enemy force.

| | |
|---|---|
| $T_0$ | Troop at base and available for tasking |
| $T_1$ | Troop tasked with reconnoitering an enemy force |
| $T_2$ | Troop tasked with engaging an enemy force in combat |

*Table 17: Significance of the* troop *CPN Places*

*BG-ATK:*

$\leftarrow C_0$
$\leftarrow R$ : reported strength = *weak*
$\rightarrow C_3$ : enemy := enemy of token in input place $R$

The *E-ATK* transition may fire when there is a commander token present in the place $C_3$ and a random amount of simulated time has elapsed. The random time delay is drawn from a negative exponential distribution with mean of $\tau_{C_3} = 1.0$ ticks. When the transition fires, the token in the place $C_3$ is consumed, a commander token is generated in the place $C_0$ and an attack order token is generated in the place $O$.

*E-ATK:*

$\leftarrow C_3$
$\rightarrow C_0$
$\rightarrow O$ : kind := *attack*, enemy := enemy of token in input place $C_3$

Where conflicts occur between transitions *BG-SR*, *BG-RCN* and *BG-ATK*, *BG-RCN* is preferred to *BG-ATK*, and *BG-SR* is preferred to *BG-RCN*.

### Initial Marking

The initial marking consists of a single token in the place $C_0$.

## 3.2.3 Troop Component

### Description

The CPN for the troop actor is shown in Figure 8. In the present simple example, there is only one troop. It would be quite straightforward to extend the model to include more than one troop by adding additional tokens to the $T_0$ place in the initial marking. The troop is assumed to be in one of three states at any one time. These are listed in Table 17 together with the symbols and identifiers used for the corresponding places.

The remaining places belong to the master net. Those places are drawn with shadows on the diagram and are passed to an instance of this net as parameters.

### Token Structure

Only one place in this subordinate CPN is not in the master CPN. That is place $T_1$. Tokens in this place have the same structure as those in places $T_0$ and $T_2$.

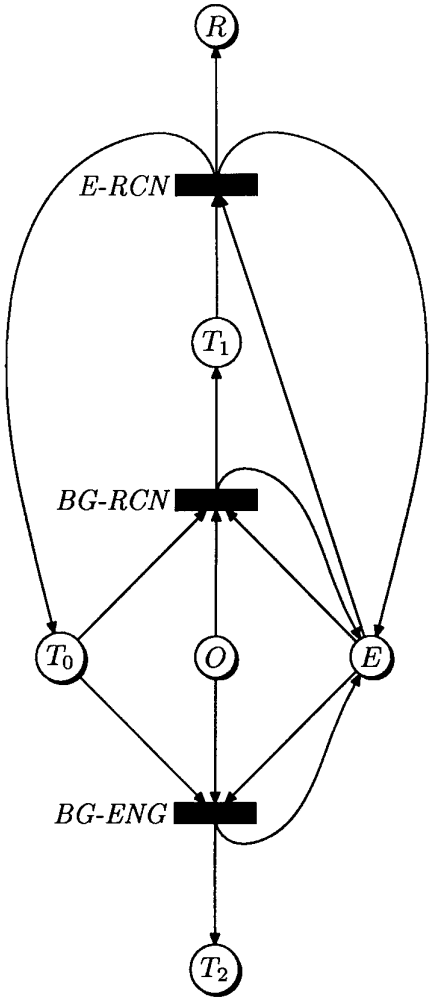



*Figure 8: Subordinate CPN for the "Troop" Component of the Command Example.*

| | |
|---|---|
| *BG-RCN* | Troop commences reconnaissance of enemy troop |
| *E-RCN* | Report on results of reconnaissance issued to commander |
| *BG-ENG* | Troop engages enemy force in combat |

*Table 18: Significance of the* troop *CPN Transitions*

### Transition Behaviour

For each of the places corresponding to the active troop states there are two transitions, one corresponding to the troop entering the state and the other to the troop leaving that state. The precondition for the *BG-RCN* transition to fire is that the troop should currently be available, that a new reconnaissance order should have been issued by the commander and that the enemy force contingent to which the order pertains should still exist within the region of operations. When the transition fires the tokens in the places $T_0$ and $O$ are consumed and a new token generated in the place $T_1$. The enemy force contingent token in place $E$ is regenerated.

*BG-RCN:*

$\leftarrow T_0$
$\leftarrow O$ : kind = *recon*
$\leftarrow E$ : enemy = enemy of token in input place $O$
$\rightarrow T_1$ : enemy := enemy of token in input place $O$
$\rightarrow E$ : enemy := enemy of token in input place $O$

The precondition for the *E-RCN* transition to fire is that a troop token occupies the place $T_1$, that the corresponding enemy token should exist and a random delay should have elapsed. The random delay time is drawn from a negative exponential distribution with a mean value of $\tau_{T_1} = 2.0$ ticks. When this transition fires, the token in the place $T_1$ is consumed and replaced with a token in the place $T_0$. The enemy force contingent token in place $E$ is regenerated.

*E-RCN:*

$\leftarrow T_1$
$\leftarrow E$ : enemy = enemy of token in input place $T_1$
$\rightarrow T_0$
$\rightarrow E$ : enemy := enemy of token in input place $T_1$
$\rightarrow R$ : $P$(reported strength|enemy strength of token in input place $T_1$) $\sim$
conditional distribution in Table 2

The *BG-ENG* transition may fire when tokens are present in the $T_0$ and $O$ places, and there is a token in the $E$ place corresponding to that in the $O$ place, indicating that the troop is not otherwise occupied, that the commander has issued a new attack order, and that the corresponding enemy exists. The troop then enters the phase of engaging the enemy in combat, which is represented by the token in the $T_0$ place being consumed and one being generated in the $T_2$ place. The token in the $O$ place is also consumed and the token in the $E$ place is regenerated as before.

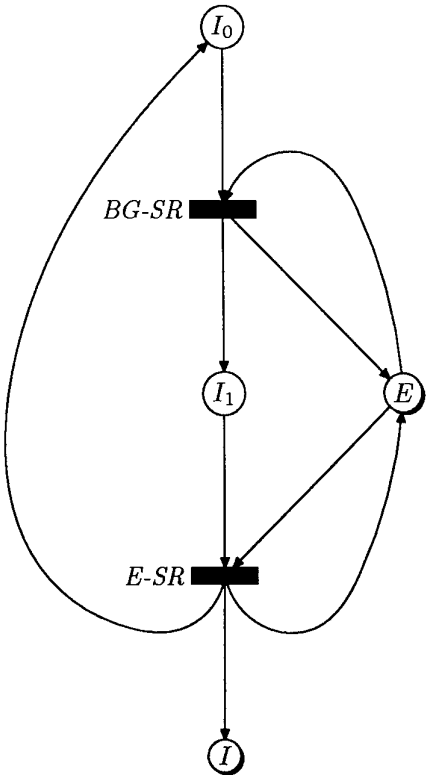



*Figure 9: Subordinate CPN for the "Intelligence Organisation" Component of the Command Example.*

*BG-ENG:*

$\leftarrow T_0$
$\leftarrow O$ : kind = *attack*
$\leftarrow E$ : enemy = enemy of token in input place $O$
$\rightarrow T_2$ : enemy := enemy of token in input place $O$
$\rightarrow E$ : enemy := enemy of token in input place $O$

### Initial Marking

The initial marking consists of a single token in the place $T_0$.

### 3.2.4 Intelligence Organisation Component

### Description

The CPN for the intelligence organisation actor is shown in Figure 9. The organisation is assumed to be in one of two states at any one time. These are listed in Table 19 together with the symbols and identifiers used for the corresponding places. The remaining

| | |
|---|---|
| $I_0$ | Intelligence organisation not occupied with equal or higher priority task |
| $I_1$ | Intelligence organisation engaged in producing situation report for commander |

*Table 19: Significance of Intelligence Organisation CPN Places*

| | |
|---|---|
| *BG-SR* | Commence the production of an enemy force situation report for the commander |
| *E-SR* | Issue a situation report to the commander |

*Table 20: Significance of Intelligence Organisation CPN Transitions*

places belong to the master net and have been passed to the subordinate net instance as parameters.

### Token Structure

The tokens in places $I_0$ and $I_1$ contain an count of the number of enemy contingents that have been reported by the intelligence organisation. The count is incremented whenever processing of a new enemy contingent is commenced. The value is transferred to the new token that is generated when processing is completed as well as the enemy contingent token that is regenerated. This allows the report tokens issued by the intelligence organisation CPN to be given a unique identifying number corresponding to the enemy contingent to which they apply. By preserving this number throughout the relevant parts of the model, tokens of other types can also be properly matched with the enemy force contingent token to which they apply. Tokens that have been processed by the intelligence organisation can be discriminated from those which have not by observing whether they have already been assigned an identifying number or not.

### Transition Behaviour

The precondition for the *BG-SR* transition to fire is that a new enemy force has been detected in the commander's region of operations (there is a new enemy force contingent token in place $E$) and that the intelligence organisation is not currently occupied by a task of equal or higher priority (the intelligence organisation token should be in place $I_0$). When the transition fires the token in the places $I_0$ is consumed and a new token generated in the place $I_1$. The token in the place $E$ is regenerated.

*BG-SR:*

$\leftarrow E$ : token not yet processed by *INTELO* actor
$\leftarrow I_0$
$\rightarrow E$ : enemy := enemy of token in input place $E$
$\rightarrow I_1$ : enemy := enemy of token in input place $E$

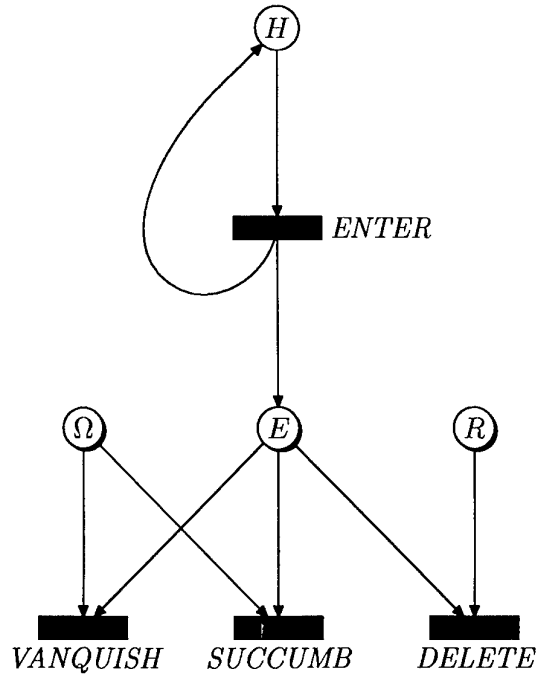



*Figure 10: Subordinate CPN for the "Enemy" Component of the Command Example.*

The precondition for the *E-SR* transition to fire is that the intelligence organisation token should occupy the place $I_1$, that a random delay should have elapsed and that there should be a matching enemy force contingent token in the place $E$. The random delay time is drawn from a negative exponential distribution with a mean value of 2.5 ticks. This corresponds to a processing rate of $\mu_I = 0.4$. When the transition fires, the token in the place $I_1$ is consumed and replaced with tokens in the places $I_0$ and $E$.

*E-SR:*

$\leftarrow E$
$\leftarrow I_1$ : enemy = enemy of token in input place $E$
$\rightarrow E$ : enemy := enemy of token in input place $E$
$\rightarrow I_0$

### Initial Marking

The initial marking consists of a single token in the place $I_0$.

## 3.2.5 Enemy Component

### Description

The CPN for the enemy actor is shown in Figure 10. The $E$ place belongs to the master CPN and is passed to the subordinate net instance as a parameter. The $H$ place is internal

| | |
|---|---|
| *ENTER* | A new enemy force enters the commander's region of operations. |
| *DELETE* | Reconnaissance report indicates that enemy force is strong. Since it will not be engaged, remove its token from further consideration. |
| *VANQUISH* | The enemy force is victorious in battle. |
| *SUCCUMB* | The enemy force succumbs in battle. |

*Table 21: Significance of Enemy CPN Transitions*

and always contains a single token that represents the fact that the enemy is presently engaged in hostilities.

### Token Structure

The only place that is not contained in the master CPN is the $H$ place. The tokens in this place have no structure. The of presence a token in place $H$ is sufficient of itself to indicate that hostilities are in progress.

### Transition Behaviour

The precondition for the *ENTER* transition to fire is that a token should be present in the place $H$ and a random time should have elapsed since it was generated. The random delay is drawn from a negative exponential distribution with a mean of 10 ticks. When the transition fires, the hostility token is regenerated in place $H$ and a new enemy force contingent token is generated in the $E$ place.

*ENTER:*

$\leftarrow H$

$\rightarrow H$

$\rightarrow E : P(\text{strength}) \sim$ probability distribution in Table 1

The precondition for the *DELETE* transition to fire is that a token should be present in place $R$ with reported enemy strength other than weak and that a token representing the same enemy should be present in place $E$. When the transition fires, both tokens are consumed and no new tokens are generated. This transition deletes enemy force contingent tokens and corresponding report tokens from the CPN for which an attack order will never be generated by the commander actor, and which would therefore otherwise remain idly in the CPN indefinitely.

*DELETE:*

$\leftarrow R$ : reported strength $\neq$ *weak*

$\leftarrow E$ : enemy = enemy of token in input place $R$

The precondition for the *SUCCUMB* transition to fire is that an enemy force contingent token should occupy the place $E$, and that there should be a corresponding combat

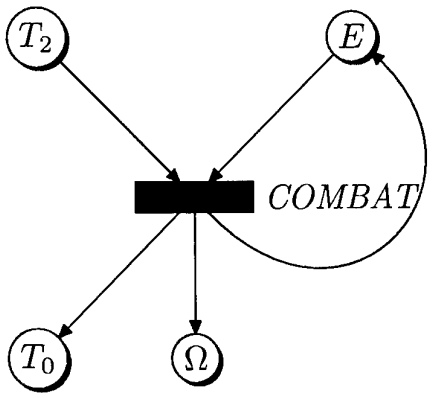



*Figure 11: Subordinate CPN for "Fate" Component of the Command Example.*

outcome token in the place $\Omega$. When this transition fires, the tokens in the place $E$ and $\Omega$ are consumed.

*SUCCUMB:*

$\leftarrow E$

$\leftarrow \Omega$ : status = *victory*, enemy = enemy of token in input place $E$

The precondition for the *VANQUISH* transition to fire is that an enemy force contingent token should occupy the place $E$, and that there should be a corresponding combat outcome token in the place $\Omega$. When this transition fires, the tokens in the place $E$ and $\Omega$ are consumed.

*VANQUISH:*

$\leftarrow E$

$\leftarrow \Omega$ : status = *defeat*, enemy = enemy of token in input place $E$

### Initial Marking

The initial marking consists of a single token in the place $H$.

### 3.2.6 Fate Component

### Description

The CPN for the fate actor is shown in Figure 11. The set of places $\{T_0, T_2, E, \Omega\}$ contained in this diagram all belong to the master CPN. The only reason for using a subordinate CPN for the fate actor is for consistency with the other actors, which are also represented by their own subordinate CPN.

### Token Structure

Since all of the places in the fate CPN are in the master CPN, their structures have already been described.

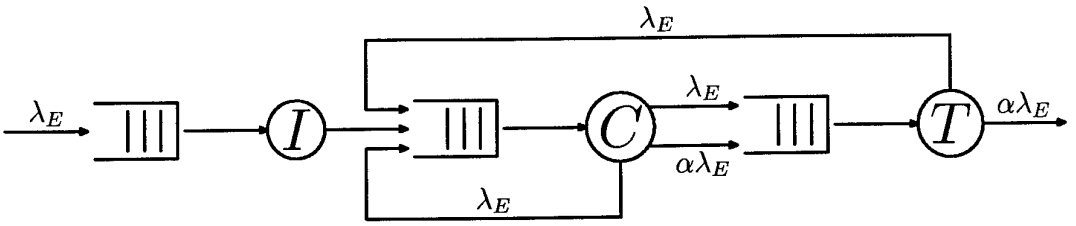



*Figure 12: Simplified Queueing Network corresponding to the CPN Model.*

### Transition Behaviour

The precondition for the *COMBAT* transition to fire is that tokens with matching enemies should be present in the $T_2$ and $E$ places, and a random time should have elapsed since the token in the place $T_2$ was generated. The random delay is drawn from a negative exponential distribution with a mean of 0.5 ticks. When this transition fires, an outcome token is generated in place $\Omega$, the troop token in place $T_2$ is consumed with another generated in place $T_0$ instead, and the enemy force contingent token is regenerated. The outcome token may have one of two subtypes: *victory*, corresponding to the case where the commander's troops are victorious; and *defeat*, where the commander's troops are defeated. The choice is made stochastically, according to the combat effectiveness conditional probabilities given in Table 3.

*COMBAT:*
$\leftarrow E$
$\leftarrow T_2$ : enemy = enemy of token in input place $E$
$\rightarrow E$ : enemy := enemy of token in input place $E$
$\rightarrow T_0$
$\rightarrow \Omega$ : $P$(status) $\sim$ probability distribution in Table 3

### Initial Marking

The initial marking has no tokens in any of the places.

## 3.3 Queueing Network Analysis

A simplified queueing network that corresponds to the CPN model described in the preceding sections is shown in Figure 12. For the case where the interarrival and service times have negative exponential distributions, this simple network can easily be solved for its steady-state behaviour. Unfortunately, queueing networks are difficult to solve in the general case. In contrast to the simple example presented here, it will in general be necessary to use Monte Carlo simulation techniques to obtain a solution.

The $I$ server has one customer type, with arrival rate $\lambda_E$ and, hence interarrival time of $1/\lambda_E$. The mean number of arrivals for some arbitrary period of time $T$ is $\overline{N} = \lambda_E T$. If the mean service time of the $I$ server is $\tau_{I_1}$, the mean time for which the server is occupied is $T_{I_1} = \overline{N}\tau_{I_1} = \lambda_E \tau_{I_1} T$. The probability of finding the server occupied at a randomly

| $i$ | $\mu_{C_i}$ | $\tau_{C_i}$ | $P(C_i)$ |
|---|---|---|---|
| 0 | - | - | 0.825 |
| 1 | 1.0 | 1.0 | 0.1 |
| 2 | 2.0 | 0.5 | 0.05 |
| 3 | 1.0 | 1.0 | 0.025 |

*Table 22: Service Rates ($\mu_{C_i}$), Service Times ($\tau_{C_i}$) and Probabilities ($P(C_i)$) for* Commander.

selected time within the period is, therefore, $P(I_1) = T_{I_1}/T = \lambda_E \tau_{I_1} = \lambda_E/\mu_I$, where $\mu_I$ is the service rate of server $I$. In order for this equation to yield a probability, the customer arrival rate must satisfy $\lambda_E \leq \mu_I$. The physical reason for this is that, if arrival rate exceeds the service rate the queue length distribution is no longer stationary. The mean queue length grows without bound. Since, from Sections 3.2.4 and 3.2.5, $\mu_I = 0.4$ and $\lambda_E = 0.1$, $P(I_1) = 0.25$ and $P(I_0) = 0.75$.

The $C$ server has three customer types. All three streams have arrival rate $\lambda_E$, however the service times for the customer types differ. In accordance with the symbology used previously, the three customer types will be designated by subscripts 1, 2 and 3. Let $\alpha$ denote the probability that reconnaissance of an enemy contingent results in a report that the enemy is weak. Then, the probabilities of finding the server serving a particular customer type at a randomly chosen instant are given by

$$\begin{aligned} P(C_1) &= \lambda_E \tau_{C_1} && (17)\\ P(C_2) &= \lambda_E \tau_{C_2} && (18)\\ P(C_3) &= \alpha \lambda_E \tau_{C_3} && (19)\\ P(C_0) &= 1 - (P(C_1) + P(C_2) + P(C_3)), && (20) \end{aligned}$$

under the condition that:

$$\lambda_E \leq \frac{1}{\tau_{C_1} + \tau_{C_2} + \alpha \tau_{C_3}}. \quad (21)$$

Using the figures in Tables 1 and 2, $\alpha = 0.7 \times 0.1 + 0.3 \times 0.6 = 0.25$. The service rates, times and probabilities for each class of customer as calculated from the formulæ above are given in Table 22. These service rates and times were given earlier as part of the model specification in Section 3.2.2.

The $T$ server has two customer types, the first with arrival rate $\lambda_E$ and the second with arrival rate $\alpha\lambda_E$. As was done earlier, these two customer types will be designated by the subscripts 1 and 2. The probabilities for this server are given by

$$\begin{aligned} P(T_1) &= \lambda_E \tau_{T_1} && (22)\\ P(T_2) &= \alpha \lambda_E \tau_{T_2} && (23)\\ P(T_0) &= 1 - (P(T_1) + P(T_2)), && (24) \end{aligned}$$

under the condition that:

$$\lambda_E \leq \frac{1}{\tau_{T_1} + \alpha \tau_{T_2}}. \quad (25)$$

| $i$ | $\mu_{T_i}$ | $\tau_{T_i}$ | $P(T_i)$ |
|---|---|---|---|
| 0 | - | - | 0.75 |
| 1 | 0.5 | 2.0 | 0.2 |
| 2 | 0.5 | 2.0 | 0.05 |

*Table 23: Service Rates ($\mu_{T_i}$), Service Times ($\tau_{T_i}$) and Probabilities ($P(T_i)$) for* Troop.

| Server | Limit |
|---|---|
| $I$ | 0.4 |
| $C$ | 0.57 |
| $T$ | 0.4 |

*Table 24: Limits on Enemy Arrival Rate*

The service rates times, and probabilities for each class of customer, as calculated from the formulæ above, are given in Table 23. These service rates and times were given earlier as part of the model specification in Sections 3.2.1 and 3.2.3.

The limits placed on the enemy arrival rate by the service times of the three servers are given in Table 24. It can be seen that, for the given scenario, the components that limit the enemy arrival rate that can be handled are the $I$ and $T$ components rather than the commander.

## 3.4 Monte Carlo Simulation

This section presents the results obtained from execution of the Petri net model. Figure 13 plots the time at which new enemy forces enter the commander's region of interest against an index which is incremented by one for each new force. Figure 14 plots the times at which the commander issues new orders to his troops against an index which is incremented by one for each new order issued. The dotted lines in both figures show the 99.7% confidence intervals.

Figures 15, 16 and 17 show plots of the total time expended in performing each of the commander, troop and intelligence organisation actor activities. The activities are numbered so as to match the numbering of the corresponding places in the CPNs for the actors. Tables 25, 26 and 27 give both the total time and the proportion of time that the actors expend in performing each activity, in numerical form.

Tables 28, 29 and 30 give the empirical statistics for the enemy force strength, troop report results and combat results. These statistics consist of the counts and the conditional relative frequencies of each outcome value. The relative frequencies may be compared with the theoretical probability values given in Tables 1, 2 and 3. Appropriate confidence limits on the counts and frequencies are derived next in Section 3.4.1.

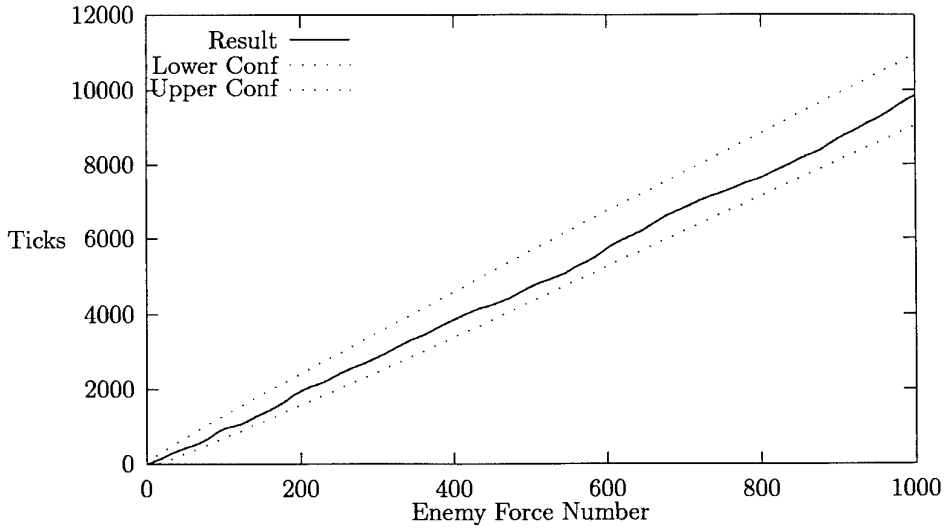



*Figure 13: Plot of Entry Times against Enemy Force Number*

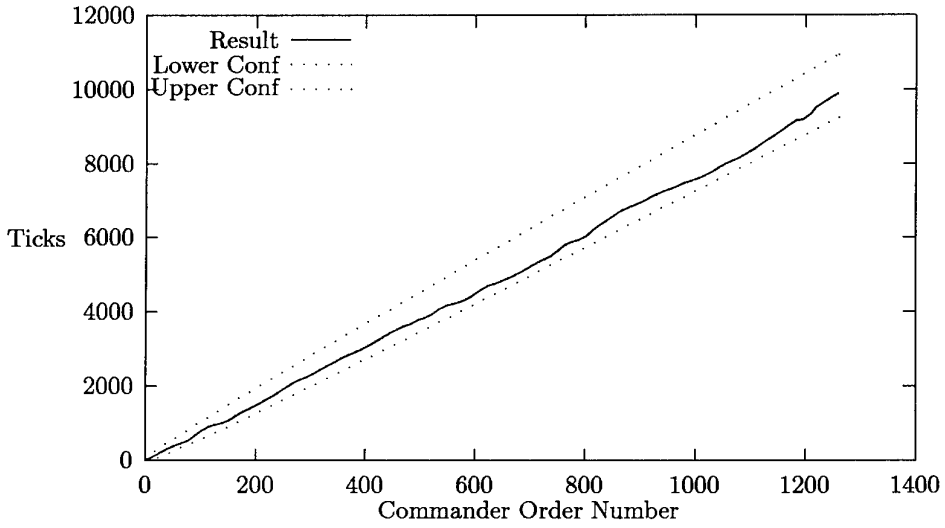



*Figure 14: Plot of Issue Times against Commander Order Number*

| State | Ticks | % |
|---|---|---|
| 0 | 7436.01 | 74.36 |
| 1 | 2563.99 | 25.64 |

*Table 25: Intelligence Organisation Activity*

| State | Ticks | % |
|---|---|---|
| 0 | 8160.63 | 81.61 |
| 1 | 1063.82 | 10.64 |
| 2 | 482.29 | 4.82 |
| 3 | 293.26 | 2.93 |

*Table 26: Command Activity*

| State | Ticks | % |
|---|---|---|
| 0 | 7533.15 | 75.33 |
| 1 | 2000.21 | 20.00 |
| 2 | 466.64 | 4.67 |

*Table 27: Troop Activity*

| Enemy Strength | |
|---|---|
| Strong | Weak |
| 724 (0.71) | 294 (0.29) |

*Table 28: Enemy Strength Statistics*

| Enemy Strength | Intelligence | | |
|---|---|---|---|
| | Strong | Unknown | Weak |
| Strong | 492 (0.68) | 158 (0.22) | 72 (0.10) |
| Weak | 38 (0.13) | 71 (0.24) | 185 (0.63) |

*Table 29: Troop Report Statistics*

| Outcome | Enemy Strength | |
|---|---|---|
| | Strong | Weak |
| Defeat | 65 (0.81) | 15 (0.19) |
| Victory | 7 (0.04) | 170 (0.96) |

*Table 30: Combat Outcome Statistics*

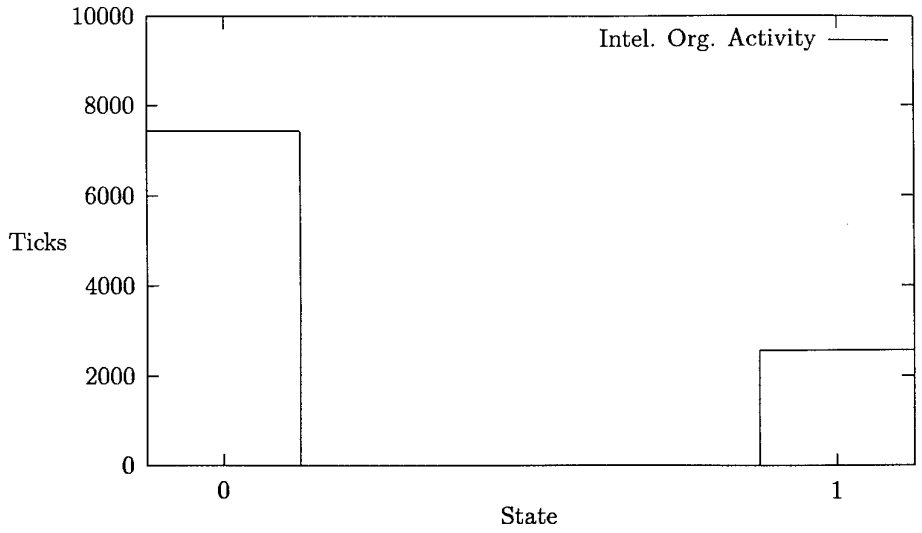



*Figure 15: Plot of Intelligence Organisation Activity*

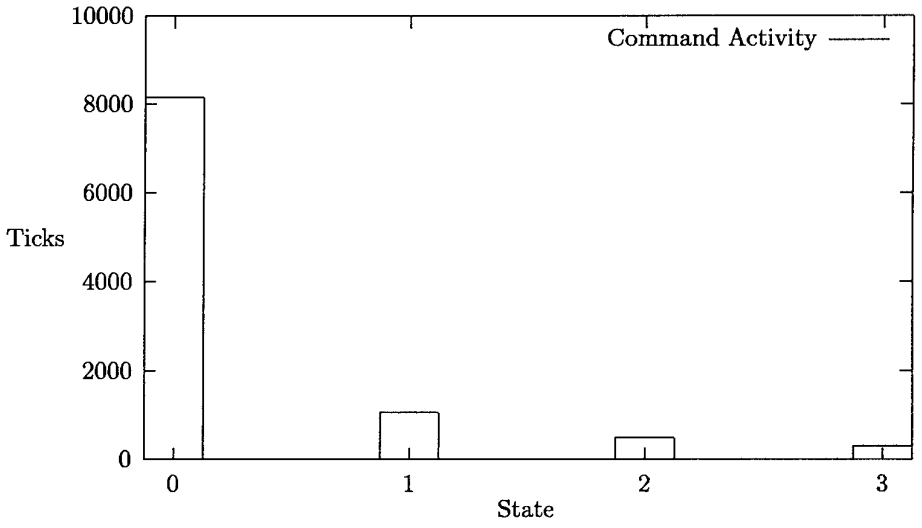



*Figure 16: Plot of Command Activity*

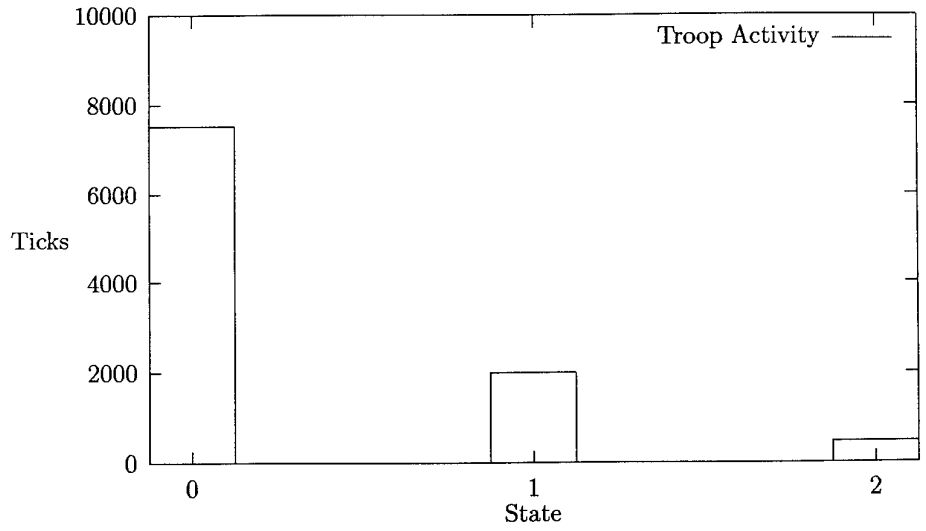



*Figure 17: Plot of Troop Activity*

### 3.4.1 Confidence Limits

In deriving confidence limits, use is made of the fact that, except for cases of vanishing probability, the results are the sum of many independent occurrences of a random variable. Therefore, on the basis of the Central Limit Theorem [2, p. 258ff.] of statistics, the distributions of the results tend towards normal distributions. Kleinrock [4, p. 338] shows that the means and variances of these distributions are given by

$$\overline{Y} = \overline{N} \cdot \overline{X} \tag{26}$$

$$\sigma_Y^2 = \overline{N}\sigma_X^2 + (\overline{X})^2\sigma_N^2, \tag{27}$$

where $\overline{Y}$ denotes the mean value of the sum of the random variables, $\overline{N}$ denotes the mean number of random variables contained in the sum, $\sigma_Y^2$ denotes the variance of the sum of the random variables, $\sigma_X^2$ denotes the variance of the individual random variables, and $\sigma_N^2$ denotes the variance of the number of random variables contained in the sum.

Let $Y$ represent the total time expended by a server having negative exponentially distributed processing time with mean $\overline{\tau}$ in processing a Poisson distributed number of customers with mean $\overline{N} = \lambda T$. The variance in number of customers for this Poisson distribution is also given by $\lambda T$. The mean of the processing time is given by $\overline{\tau}$ and its variance is given by $\overline{\tau}^2$. Consequently, the mean and variance for the total processing time are given by

$$\overline{Y} = \lambda T\overline{\tau} \tag{28}$$

$$\sigma_Y^2 = 2\lambda T\overline{\tau}^2. \tag{29}$$

The result in Equation 28 was applied earlier without justification in Section 3.3. This section has now provided a justification for it. The confidence limits for each server state, except for the idle state, can be calculated using the variance obtained from Equation 29.

| State | Limits | % |
|---|---|---|
| 0 | $7500 \pm 335$ | $75.00 \pm 3.35$ |
| 1 | $2500 \pm 335$ | $25.00 \pm 3.35$ |

*Table 31: Intelligence Organisation Activity Limits*

| State | Limits | % |
|---|---|---|
| 0 | $8250 \pm 268$ | $82.50 \pm 2.68$ |
| 1 | $1000 \pm 134$ | $10.00 \pm 1.34$ |
| 2 | $500 \pm 67$ | $5.00 \pm 0.67$ |
| 3 | $250 \pm 67$ | $2.50 \pm 0.67$ |

*Table 32: Command Activity Limits*

The variance for the idle state is simply the sum of the variances of the other states. Hence confidence limits for the idle state can also easily be calculated.

Now, instead, let $Y$ represent the total number of events which occur when each customer has a probability $p$ of causing an event to occur. Then $Y$ is the sum of independent discrete random variables taking the value 0 with probability $1-p$ and taking the value 1 with probability $p$. The mean value for each random variable is just $p$, while the variance is $p - p^2$. Substituting these values into Equations 26 and 27 gives

$$\overline{Y} = \lambda T p \tag{30}$$

$$\sigma_Y^2 = \lambda T p. \tag{31}$$

This is what would be intuitively expected as the result is effectively a Poisson process with parameter $\lambda p$. Again, this expression was used without justification in Section 3.3 and has now been justified here.

Confidence limits of $\pm 3\sigma$ for the total time and fraction of time the actors spend performing each activity are given in Tables 31, 32 and 33. Similar confidence limits for the enemy strength, troop report and combat outcome statistics and frequencies are given in Tables 34, 35 and 36. The limits of $\pm 3\sigma$ used above correspond to a confidence level of 99.7%.

| State | Limits | % |
|---|---|---|
| 0 | $7500 \pm 402$ | $75.00 \pm 4.02$ |
| 1 | $2000 \pm 268$ | $20.00 \pm 2.68$ |
| 2 | $500 \pm 134$ | $5.00 \pm 1.34$ |

*Table 33: Troop Activity Limits*

| Enemy Strength | |
|---|---|
| Strong | Weak |
| $700 \pm 79$ $(0.70 \pm 0.08)$ | $300 \pm 52$ $(0.30 \pm 0.05)$ |

*Table 34: Enemy Strength Count (Frequency) Limits*

| Enemy Strength | Intelligence | | |
|---|---|---|---|
| | Strong | Unknown | Weak |
| Strong | $490 \pm 66$ $(0.70 \pm 0.09)$ | $140 \pm 35$ $(0.20 \pm 0.05)$ | $70 \pm 25$ $(0.10 \pm 0.04)$ |
| Weak | $45 \pm 20$ $(0.15 \pm 0.07)$ | $75 \pm 26$ $(0.25 \pm 0.09)$ | $180 \pm 40$ $(0.60 \pm 0.13)$ |

*Table 35: Troop Report Count (Frequency) Limits*

## 3.5 Temporal Effects of Information Warfare

Now that a scenario model which is capable of incorporating temporal effects has been developed and demonstrated, it will be applied to analysis of the effectiveness of IW options which rely on temporal effects. Monte Carlo methods will not be employed because, for the simple case considered here, the required results can easily be derived by means of Queueing Network Analysis. This permits a wide range of parameters to be quickly and conveniently explored. The Monte Carlo method would be more cumbersome for this purpose.

### 3.5.1 Information Delay

This section considers the effect of delaying the intelligence information reaching the commander. It will be assumed that the enemy contingent's sojourn time in the commander's region of operations is negative-exponentially distributed with a mean time of $\tau_S$. For the results computed here, it will be assumed that $\tau_S = 50.0$.

The processing delay is composed of two parts. The first part is the time spent awaiting the attention of the server for the stage. This is the *queueing time*. The second part is the time spent being processed by the server, which is the *processing time*. Kleinrock [4] terms the sum of these two times the *system time*. The same name will be used here.

As before, it is assumed that the interarrival times for the individual customer types, $i$, are negative-exponentially distributed with arrival rates $\lambda_i$, and that their processing times are also negative-exponentially distributed, with processing rates $\mu_i$. Let $\lambda = \sum_{i=1}^{n} \lambda_i$.

| Outcome | Intelligence | |
|---|---|---|
| | Strong | Weak |
| Defeat | $63 \pm 24$ $(0.90 \pm 0.34)$ | $18 \pm 13$ $(0.10 \pm 0.07)$ |
| Victory | $7 \pm 8$ $(0.10 \pm 0.11)$ | $162 \pm 38$ $(0.90 \pm 0.21)$ |

*Table 36: Outcome Count (Frequency) Limits*

Then $\lambda_i/\lambda$ is the probability that an arbitrary arrival is of type $i$. Therefore, the processing time distribution, $b(t)$, for such an arrival is given by

$$b(\tau) = \sum_{i=1}^{n} \alpha_i e^{-\mu_i \tau}, \tag{32}$$

where $\alpha_i = \lambda_i/\lambda$. Thus, the processing time distribution is hypergeometric. This distribution is denoted by the letter $H$ in queueing theory.

According to Kleinrock [4, p. 190], the mean queueing time for a "customer" in an $M/G/1$ queue, including $M/H_n/1$ queues such as those used here, is given by

$$W = \frac{\rho\bar{\tau}(1 + C_b^2)}{2(1 - \rho)} \tag{33}$$

where $\bar{\tau}$ denotes the mean processing rate, $C_b^2 = \sigma_b^2/\bar{\tau}^2 = (\overline{\tau^2}/\bar{\tau}^2) - 1$ denotes the squared coefficient of variation of the processing time, and $\rho = \lambda\bar{\tau}$ denotes the server utilisation.

It is assumed that all customers in the queue are treated identically, regardless of type. The mean system time for a customer of type $i$ is then given by the sum of the mean time spent queueing by the customer plus the mean processing time for customers of type $i$. This is simply given by

$$T_i = \tau_i + W, \tag{34}$$

where $\tau_i = 1/\mu_i$.

The mean processing time $\bar{\tau}$ for a hypergeometric server having $n$ alternative service rates, $H_n$, is given by

$$\bar{\tau} = \sum_{i=1}^{n} \alpha_i \tau_i. \tag{35}$$

This can be expressed in terms of the probability, $p_0$, that the server is idle as:

$$\bar{\tau} = \frac{1 - p_0}{\lambda}. \tag{36}$$

Then $\rho$ can be expressed as $\rho = \lambda\bar{\tau} = 1 - p_0$, and the expression for the queueing time becomes:

$$W = \frac{(1 - p_0)^2(1 + C_b^2)}{2\lambda p_0}. \tag{37}$$

The second moment of the processing time is given by

$$\overline{\tau^2} = 2\sum_{i=1}^{n} \alpha_i \tau_i^2. \tag{38}$$

Therefore, the squared coefficient of variation of the processing time distribution, $C_b^2$, is given by

$$C_b^2 = \frac{2\sum_{i=1}^{n} \alpha_i \tau_i^2}{\left(\sum_{i=i}^{n} \alpha_i \tau_i\right)^2} - 1 \tag{39}$$

The mean processing time, idle probability and mean system time for each of the processing stages are given in Table 38. Consequently, mean processing delay in the entire

| Server | $p_0$ | $C_b^2$ | $W$ |
|---|---|---|---|
| $I$ | 0.75 | 1.0 | 0.833 |
| $C$ | 0.825 | 2.02 | 0.182 |
| $T$ | 0.75 | 1.0 | 0.667 |

*Table 37: Queueing Times*

| $i$ | Stage | $\tau_i$ | $(W)_i$ | $T_i$ |
|---|---|---|---|---|
| 1 | $I_1$ | 2.5 | 0.833 | 3.33 |
| 2 | $C_1$ | 1.0 | 0.182 | 1.18 |
| 3 | $C_2$ | 0.5 | " | 0.682 |
| 4 | $C_3$ | 1.0 | " | 1.18 |
| 5 | $T_1$ | 2.0 | 0.667 | 2.67 |
| 6 | $T_2$ | 2.0 | " | 2.67 |

*Table 38: Service Stage Times*

system is $T_\Sigma = T_1 + T_2 + T_3 + T_5 + \alpha(T_4 + T_6)$, where, as before, $\alpha = 0.25$ denotes the probability that a decision is made to attack. Hence, $T_\Sigma = 8.83$. Applying Little's result (see [4, p. 17]), the mean number of enemy contingents being processed at any one time by the entire organisation is:

$$\begin{aligned} \overline{N} &= \lambda_E T_\Sigma \\ &= 0.883. \end{aligned} \tag{40}$$

Let $F_\delta(d)$ denote the probability distribution function of the difference between the sojourn time of the enemy in the commander's region of operation and the processing delay for the enemy. Define $d$ to be positive when the sojourn times exceeds the processing delay and negative otherwise. Then $F_\delta(d)$ is the probability that the enemy evades contact if an additional delay $d$ is introduced into the processing. It will be assumed that this additional delay is due to an IO which delays the receipt of intelligence from the intelligence organisation by the commander.

It is assumed that the system has achieved steady-state equilibrium and that, therefore, the service stage durations are independent of each other, and are also independent of the enemy sojourn time in the region. Whether this is a realistic assumption or not will depend on whether the situation being modelled is a protracted one or is short-lived. Denote the probability density function of the total system time by $f_\Sigma(t)$, the probability distribution and probability density functions of the enemy sojourn time by $F_S(t)$ and $f_S(t)$, respectively, and the joint density function of the enemy sojourn time and the total system time by $f_{S\Sigma}(t,\tau)$. Then:

$$\begin{aligned} F_\delta(d) &= \int_{-\infty}^{\infty}\int_{-\infty}^{\tau+d} f_{S\Sigma}(t,\tau)dtd\tau \\ &= \int_{-\infty}^{\infty}\int_{-\infty}^{\tau+d} f_S(t)f_\Sigma(\tau)dtd\tau \end{aligned}$$

$$= \int_{-\infty}^{\infty} F_S(\tau + d) f_\Sigma(\tau) d\tau, \tag{41}$$

where:

$$F_S(t) = 1 - e^{-\lambda_S t}. \tag{42}$$

The probability density function for the total system time, $f_\Sigma(t)$, is given by the convolution of the probability density functions of the system times of the individual stages. Denote the densities of the individual system times by $f_i(t)$, $i = 1, \ldots, 6$. Then:

$$f_\Sigma(t) = \bigotimes_{i=1}^{6} f_i(t). \tag{43}$$

Taking the Laplace transform of both sides of Equation 43 therefore gives:

$$\hat{f}_\Sigma(s) = \prod_{i=1}^{6} \hat{f}_i(s). \tag{44}$$

An expression for the Laplace transform of the system time probability density for a single stage is derived in Appendix B. The result is given in Equation B4. The system time density transforms for the individual stages are substituted into Equation 44 to obtain an expression for the Laplace transform of the total system time in terms of the parameters of the individual distributions. $F_\delta(d)$ may then be calculated by inverting Equation 44, and substituting the result, together with Equation 42, into Equation 41.

If the delay $d$ is deterministic, the required probability can be obtained by directly inserting the value of $d$ into the final expression. However, if the delay is a random variable, then the expected value of the expression with respect to the distribution of $d$ must be computed. Here it will be assumed that the delay is deterministic. Some tabulated results for the probability of the enemy eluding contact for various value of the delay are given in Table 39. The value for $d = 0$ corresponds to the case of no IO.

Now that the enemy sojourn time is considered to be limited, there is a finite probability of evasion, even when no IO is undertaken. Let $p_e$ denote this evasion probability. Furthermore, let $p'_e$ denote the probability of evasion when IO is undertaken, and $\Delta p_e = p'_e - p_e$ the increase in evasion probability when IO is undertaken. Then the decrease in the commander's satisfaction due to the IO for the decision policy given in Section 2.6 is $P(I = \mathit{Weak})E[U|I = \mathit{Weak}]\Delta p_e = 18\Delta p_e$. This gives the effectiveness of the operation, which will be denoted by $\epsilon(d, 0)$. The effectiveness of the IO for the various values of $d$ is also shown in Table 39. The result of plotting a smooth curve through the effectiveness values is shown in Figure 18.

### 3.5.2 Prolonged Decision Making

The case of prolonged decision making can be treated in the same way as the case of information delay described in Section 3.5.1. However, now it is assumed that $d$ is fixed at zero and a parameter corresponding to the commander's decision making time is varied instead. It is assumed that it is primarily the mean time required for the commander to produce reconnaissance orders that is affected by the IO. This parameter will be denoted

| $d$ | $p'_e = F_\delta(d)$ | $\epsilon(d,0)$ [Utiles] |
|---|---|---|
| 0 | 0.204 | 0 |
| 2.5 | 0.243 | 0.702 |
| 5 | 0.280 | 1.37 |
| 10 | 0.349 | 2.61 |
| 20 | 0.467 | 4.73 |
| 30 | 0.563 | 6.46 |
| 40 | 0.643 | 7.90 |
| 50 | 0.707 | 9.05 |

*Table 39: Evasion Probability and Effectiveness for Delayed Information*

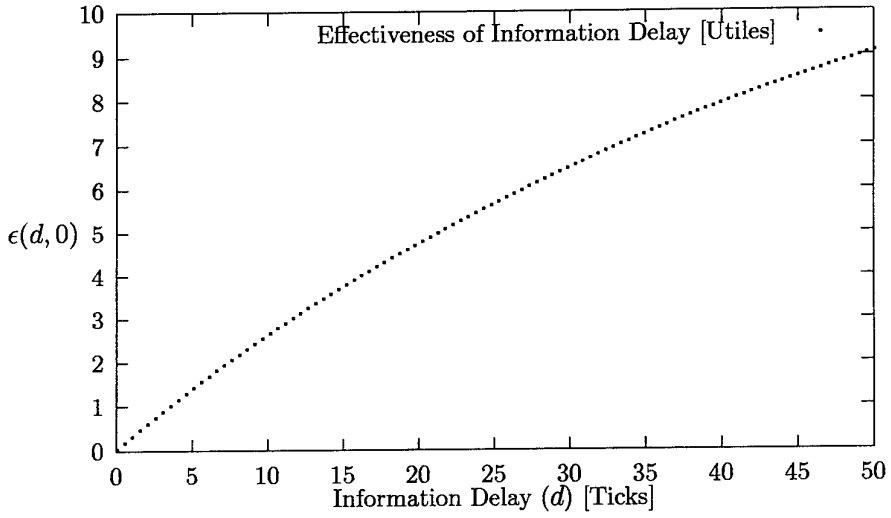



*Figure 18: Plot of Effectiveness of Information Delay*

| $\beta$ | $\Delta\beta$ | $p'_e = F_\delta(0)\|_{\tau_3=\beta}$ | $\epsilon(0,\Delta\beta)$ [Utiles] |
|---|---|---|---|
| 0.5 | 0 | 0.204 | 0 |
| 1.0 | 0.5 | 0.217 | 0.234 |
| 2.0 | 1.5 | 0.253 | 0.882 |
| 3.0 | 2.5 | 0.307 | 1.85 |
| 4.0 | 3.5 | 0.382 | 3.2 |
| 5.0 | 4.5 | 0.485 | 5.06 |
| 6.0 | 5.5 | 0.622 | 7.52 |
| 7.0 | 6.5 | 0.791 | 10.6 |
| 8.0 | 7.5 | 0.955 | 13.5 |
| 8.74 | 8.24 | 0.999999 | 14.3 |

*Table 40: Evasion Probability and Effectiveness for Prolonged Decision Making*

by the symbol $\beta$. The value of the parameter for the case of no IO will be denoted by $\beta_0$. Then the mean prolongation time will be given by $\Delta\beta = \beta - \beta_0$. The enemy's probability of evading contact will be examined for $\Delta\beta \geq 0$. The effectiveness of the IO, $\epsilon(0,\Delta\beta)$, is the decrease in the commander's satisfaction that it produces.

The case of prolonged decision making differs significantly from that of information delay in that, if the prolongation time can be made sufficiently large, the commander can no longer keep up with the rate at which new enemy contingents arrive. For the example presented here, this phenomenon occurs for $\beta = 8.75$ or $\Delta\beta = 8.25$. In the simple model used for the example, this causes the system time to grow indefinitely large as the queue length increases with time. As a result, the enemy is almost certain to evade contact after the situation has persisted for some time. In practice, of course, the queue length would be managed in some way to ensure that its length remained tolerable, such as by discarding stale or *senescent* members, that is old unprocessed members for which it is likely to be too late to take action. Such issues concerning queueing discipline are not analysed further here.

Some tabulated results for the probability of the enemy eluding contact and for the effectiveness of the IO for various values of this parameter $\Delta\beta$ are given in Table 40. The case $\beta = 0.5$ corresponds to no IO. The result of plotting a smooth curve through the effectiveness values is shown in Figure 19.

## 3.6 Summary

This section has demonstrated the analysis of the temporal effects of IO. It has presented a hierarchical, stochastic CPN model of the simple Military Command Organisation used as an example in the previous sections. The model used in this section has a few additional embellishments that were previously irrelevant.

Two solution techniques for the temporal behaviour of the model have been demonstrated. The first was Monte Carlo simulation, which is a generally applicable technique. However, it is sometimes more convenient to use techniques that based on Queueing Network Analysis, especially for simple models such as the one used here. This is particularly

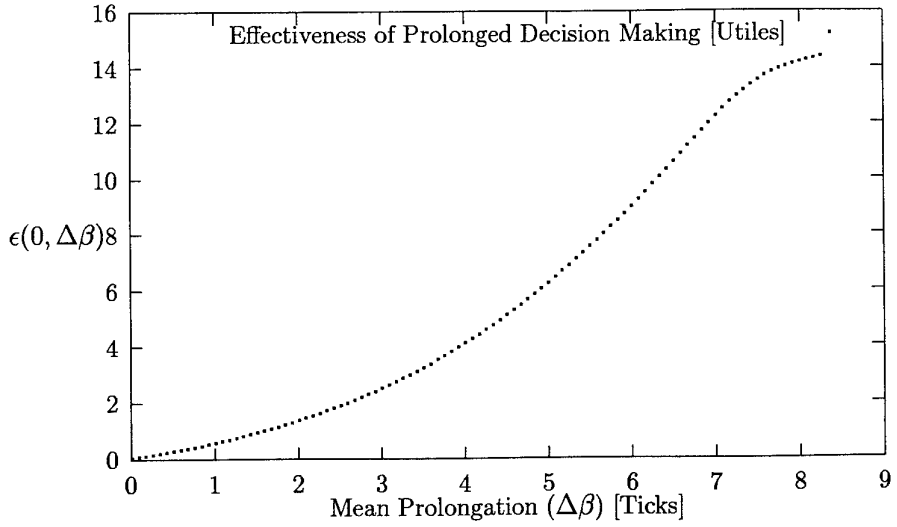



*Figure 19: Plot of Effectiveness of Prolonged Decision Making*

so when it is desired to evaluate some effectiveness measure for a range of parameter values. If the Monte Carlo method were used, it would require the simulation to be repeated for each value of the parameter of interest. Another difficulty with the Monte Carlo method is that, because it is based on computing statistical averages, it can be computationally expensive to achieve tight confidence bounds.

In this section interest has been focussed on the relationship between effectiveness and additional information delay, as well as that between effectiveness and decision time prolongation. A theoretical analysis based on an approximation was sufficient for present purposes. Plots of the relationships of interest were given in Figures 18 and 19. These demonstrate, for example, that effectiveness is more sensitive to decision time prolongation than to increase in information delay. This is obviously so because as the command decision cycle time is lengthened, a point is eventually reached at which a backlog develops which grows indefinitely and therefore prevents timely decisions from being made.

If greater accuracy were required than that achieved by the approximate theoretical analysis, it would be necessary to employ numerical analysis techniques based on Markov Chain theory, if the Monte Carlo method was to be avoided. Such analyses tend to be very complex because the state space of the Markov model that must be considered in order to obtain accurate results is very large. A number of software tools for assisting the Markov chain analysis of stochastic Petri nets appear to exist. However, they are mainly the result of research development, rather than commercial grade products.

# 4 Conclusion

This report has demonstrated that the effectiveness of wide variety of IO related to IW can be reduced to a common measure. The importance of this is that the effectiveness of IO

of differing kinds can be directly compared. Furthermore, the same effectiveness measure could be applied to conventional operations, thus allowing conventional operations and IO to be directly compared.

The proposed effectiveness measure is, however, both abstract and subjective. It is the change in the level of satisfaction experienced by the commander against whom the IO is directed. This is expressed quantitatively in a subjective unit of measure termed the "Utile", which has its origins in Decision Theory. Different commanders may assign divergent values to the effectiveness for the same operation. The degree of divergence found would be expected to depend on the level and commonality of training that these commanders have received. A more highly trained cohort would be expected to give a smaller divergence than a less highly trained one, because training would be expected to instill common values.

The measure is most readily applied in a defensive context. In that case, the operation would be a hypothetical one and the objective would be to assess the susceptibility of a commander of one's own forces to such an attack. It would be expected that the commander would cooperate in the establishment of an appropriate satisfaction scale. Ideally, he would be able to do this himself, with minimal external assistance, using an appropriate software tool. In an offensive context, the enemy commander's satisfaction scale would need to be determined by some indirect means, which would make the analysis more difficult and uncertain.

In order to permit selection of the appropriate analysis techniques, the IO considered have been divided into two main categories, according the type of effect produced. Those which produce effects which do not explicitly depend on a time parameter have been termed *secular*. These can be analysed using decision trees or Influence Diagrams. Examples of secular operations are those resulting in information denial, those creating a deception, and psychological operations. Those operations which produce effects that explicitly depend on a time parameter have been termed *temporal*. These require additional tools for analysis. Examples of temporal operations are those resulting in increased information delay and in prolonged decision-making time. The five subordinate classes of IO listed above may be considered to cover all types of IO relevant to IW, that is to hostilities conducted in the information domain.

The primary temporal modelling tool that has been used in this report is the Stochastic CPN. A number of techniques exist for analysing the stochastic properties of CPNs. The most straightforward and direct is Monte Carlo simulation, and a demonstration of the use of this technique has been given in the report. However, other analysis techniques can be convenient. An example is given in the report of the application of Queueing Network Analysis to a queueing network derived from the CPN model. Theoretical results based on an approximation were sufficient for present purposes. If greater accuracy were required, it would be necessary to employ numerical analysis techniques based on Markov Chain theory. Such analyses tend to be very complex because the state space of the Markov model that must be considered in order to obtain accurate results is very large. Therefore, Monte Carlo simulation is likely to be the preferred technique in general.

# References


1. Peter Checkland and Sue Holwell. *Information, Systems and Information Systems - making sense of the field.* John Wiley & Sons, 1998.

2. William Feller. *An Introduction to Probability Theory and Its Applications*, volume II. John Wiley & Sons, 2nd edition, 1971.

3. Ralph L. Keeney. *Decisions with Multiple Objectives: Preferences and Value Tradeoffs.* John Wiley and Sons, 1976.

4. Leonard Kleinrock. *Queueing Systems*, volume 1. John Wiley & Sons, 1975.

5. Alexander H. Levis. Object oriented design of decision making organisations. In A. H. Levis, editor, *The Science of Command and Control: Part III, Coping with Change.* AFCEA International Press, 1994.

6. James E. Matheson. Using influence diagrams to value information and control. In Robert M. Oliver, editor, *Influence Diagrams, Belief Nets and Decision Analysis*, chapter 2. John Wiley & Sons, 1990.

7. Daniel T. Maxwell. Supporting decision-makers in future conflicts: A decision theoretic persepective. In Alexander Woodcock, editor, *Analytic Approaches to the Study of Future Conflict*, pages 206–226. The Canadian Peacekeeping Press, 1996.

8. R. E. Neapolitan. *Probabilistic Reasoning in Expert Systems: Theory and Algorithms.* John Wiley and Sons, 1990.

9. Norsys Software Corp, 2315 Dunbar Street, Vancouver, Canada, V6R 3N1. *Netica Application User's Guide, Version 1.05*, March 1997.

10. Judea Pearl. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference.* Morgan Kaufmann Publishers, 1997.

11. Didier Perdu. Effectiveness of two modes of information pull in the Copernicus architecture. In A. H. Levis, editor, *The Science of Command and Control: Part III, Coping with Change.* AFCEA International Press, 1994.

12. Howard Raiffa. *Decision Analysis: Introductory Lectures on Choices under Uncertainty.* Behavioral Science: Quantitative Methods. Addison-Wesley, 1968.

13. Brian S. Ray. Crisis management in the national military command center (NMCC). In A. H. Levis, editor, *The Science of Command and Control: Part III, Coping with Change.* AFCEA International Press, 1994.

14. C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(379–423, 623–656), 1948.

15. Roderick J. Staker. Information system network risk analysis using Bayesian belief networks. Technical Report DSTO-TR-0830, DSTO, Electronics and Surveillance Research Laboratory, PO Box 1500, Salisbury, South Australia, 5108, Australia, June 1999.

16. John von Neumann. *Theory of Games and Economic Behaviour.* Science Editions. John Wiley & Sons, 1964.

17. Edward Waltz. *Information Warfare: Principles and Operations.* Artech House, Inc., 1998.

# Appendix A
# Removing a Random Variable from a Decision Tree by Marginalisation

The appendix describes the mathematical details involved in removing the *Enemy Strength* random variable from the Decision Tree discussed in Section 1.2.1.

Define a value function $f$ so that the satisfaction value associated with decision $d$ when the enemy strength is $s$ is given by

$$u = f(d, s). \tag{A1}$$

The value $u$ does not depend on the *Intelligence* random variable because that random variable provides no additional information, once the actual enemy strength is given. Let $S$ denote the *Enemy Strength* random variable and $U$ the corresponding value random variable:

$$U = f(d, S). \tag{A2}$$

Using Bayes' rule, the conditional expectation of $U$, when the value of the decision variable $D$ is $d$ and the value of the intelligence random variable $I$ is $i$, is:

$$\begin{aligned} E[U|I = i, D = d] &= \sum_s f(d, s) P(S = s|I = i) \\ &= \frac{\sum_s f(d, s) P(S = s, I = i)}{P(I = i)}. \end{aligned} \tag{A3}$$

In addition, the marginal probability that the value of the intelligence random variable is $i$ is:

$$\begin{aligned} P(I = i) &= \sum_s P(S = s, I = i) \\ &= \sum_s P(I = i|S = s) P(S = s). \end{aligned} \tag{A4}$$

This enables the conditional expectations to be calculated from the known quantities $P(S = s)$, $P(I = i|S = s)$ and $f(d, s)$. In fact these are just the quantities that are labelled on the original decision tree. The values of $P(S)$ label the arms of the first fork, those of $P(I|S)$ the arms of the subsequent set of forks, and those of $f(d, s)$ the arms of the last set of forks.

The marginalised, or folded, Decision Tree has only the initial three-way fork, corresponding to the possible values of the intelligence random variable, followed by a subsequent set of two-way forks corresponding to the commander's decision. The arms the intelligence forks are labelled with the marginal probabilities of the intelligence values to which they correspond, as calculated from the original tree using Equation A4. The decision forks are labelled with the conditional expectations calculated from Equation A3.

Let $D^*(i)$ denote the optimal decision, i.e., the one yielding the highest satisfaction, for the marginalised, or "folded", decision tree, when the value of the intelligence random

variable is $i$. The optimal decision policy can only depend on the intelligence value since the enemy strength is unobservable in the folded Decision Tree. The expected value of $U$ for this optimal decision policy is:

$$E^*[U] = \sum_i E[U|I = i, D = D^*(i)]P(I = i). \tag{A5}$$

This relation can be proven by substituting Equation A3 into Equation A5 and noting that the result coincides with the definition of conditional expectation.

# Appendix B
# Derivation of System Time Density Transform

Consider a server $S$ which processes a queue of customers arriving from several independent sources with negative exponentially distributed arrival times. Suppose that the interarrival time distribution for each source is different and that the parameters of these are $\lambda_i$. The probability of an arrival to the queue in a small time interval $\Delta t$ is given by $\lambda \Delta t$, where $\lambda = \sum_i \lambda_i$. Consequently the interarrival time distribution for arrivals to the queue, regardless of source, is negative exponential with parameter $\lambda$.

Suppose that the server processes the customers at a rate $\mu_i$ which is dependent on the source from which the customer arrived. The source is taken to correspond to the type of customer and hence the stage of processing that is required. Under these conditions, the processing time density, $b(t)$, for a customer is given by

$$\begin{aligned} b(t) &= \sum_i \alpha_i b_i(t) \\ &= \sum_i \alpha_i \mu_i e^{-\mu_i t}, \end{aligned} \tag{B1}$$

where $\alpha_i$ is the probability that the customer being serviced is of type $i$, and $b_i(t)$ is the processing time density for the $i$-th customer type. Clearly, by the application of flow conservation principles, the $\alpha_i$ are simply the relative frequencies of arrival of the different customer types, and are given by $\alpha_i = \lambda_i / \lambda$.

Let $p_i$, $i > 0$, be the probability that the server is processing a customer of type $i$ at a randomly chosen instant, and let $p_0$ be the probability that the server is idle at a randomly chosen instant. Then $\rho = 1 - p_0 = \sum_{i>0} p_i$ is the server utilisation factor. It was previously shown in Section 3.3 that $p_i = \lambda_i \tau_i = \lambda_i / \mu_i$, $i > 0$, by considering mean values over an extended period of time.

The queue can be considered to be a simple $M/G/1$ queue having Poisson arrivals with an arrival rate $\lambda$ and having a processing time distribution $b(t)$. (In fact the queue is of the more specialised $M/H_n/1$ type, where the $H$ denotes a hypergeometric processing time distribution.) According to Kleinrock [4, §5.7], the Laplace transform of the queueing time density for such a queue, $\hat{w}(s)$, is:

$$\hat{w}(s) = \frac{s(1-\rho)}{s - \lambda + \lambda \hat{b}(s)}, \tag{B2}$$

where $\hat{b}(s)$ is the Laplace transform of the processing time probability density function. Taking the Laplace transform of Equation B1, $\hat{b}(s)$ is given by

$$\begin{aligned} \hat{b}(s) &= \sum_i \alpha_i \hat{b}_i(s) \\ &= \sum_i \frac{\alpha_i \mu_i}{s + \mu_i}. \end{aligned} \tag{B3}$$

While all customer types experience the same queueing time distribution, the *system time* will be different for different types of customer. Assuming that the queueing time and processing time are independent, the Laplace transform of the system time density for customers of type $i$, $\hat{f}_i(s)$, is given by

$$\begin{aligned}\hat{f}_i(s) &= \hat{w}(s)\hat{b}_i(s) \\ &= \hat{b}_i(s)\frac{s(1-\rho)}{s-\lambda+\lambda\hat{b}(s)} \\ &= \frac{\mu_i s(1-\rho)}{(\mu_i+s)(s-\lambda+\lambda\hat{b}(s))}.\end{aligned} \tag{B4}$$

The difficulty with using this result for the queueing network in Section 3.3 is that the interdeparture time distribution for the queue is not negative exponential. This means that queues down-stream of the $C$ server are no longer of the $M/G/1$ type. Furthermore, since the output of the $C$ server feeds back into its own input queue, this queueing system cannot be $M/G/1$ either. According to Kleinrock [4, §4.8], the Laplace transform of the interdeparture time is given by

$$\hat{d}(s) = \left[(1-\rho)\left(\frac{\lambda}{s+\lambda}\right)+\rho\right]\hat{b}(s). \tag{B5}$$

The mean interdeparture time can be obtained from:

$$\bar{\tau}_d = -\frac{d}{ds}\hat{d}(s)\bigg|_{s=0}. \tag{B6}$$

This can be evaluated using a symbolic algebra system such as Maxima. For $i = 2$, for example, the result is:

$$\bar{\tau}_d = \frac{1}{\lambda_1+\lambda_2}. \tag{B7}$$

This equation must also hold from conservation of flow considerations so the result provides a check that the derivation is correct.

The variance of the interdeparture time can be obtained from:

$$\begin{aligned}\sigma^2_{\tau_d} &= \overline{\tau_d^2} - \bar{\tau}_d^2 \\ &= \frac{d^2}{ds^2}\hat{d}(s)\bigg|_{s=0} - \bar{\tau}_d^2 \\ &= \frac{1+2\frac{\lambda_1}{\mu_1}\frac{\lambda_2}{\mu_2}\left(\frac{\mu_2}{\mu_1}-1\right)\left(1-\frac{\mu_1}{\mu_2}\right)}{(\lambda_1+\lambda_2)^2}.\end{aligned} \tag{B8}$$

The first term in the numerator corresponds to the variance that a negative exponential interdeparture time process would have. The second term is small if $\lambda_1/\mu_1$ and $\lambda_2/\mu_2$ are small and, in addition, $\mu_1$ and $\mu_2$ are comparable. Of course, when the two processing rates are identical, the second term vanishes, as would be expected. For the purpose of the demonstration example presented in this report, where great accuracy is not required, it will be assumed that the interdeparture times can be treated as negative-exponentially distributed processes, and that Equation B4 can therefore be validly used for the down-stream stages.

Military Information Operations Analysis Using Influence Diagrams And Coloured Petri Nets

*(R. J. Staker)*

(DSTO–TR–0914)

DISTRIBUTION LIST

| | Number of Copies |
|---|---|
| **DEFENCE ORGANISATION** | |
| **Task Sponsor** | |
| Director General Information Strategic Concepts, M-SB-43, Department of Defence, Canberra ACT 2600 | 1 |
| **S&T Program** | |
| Chief Defence Scientist<br>FAS Science Policy<br>AS Science Corporate Management | 1 |
| Director General Science Policy Development | 1 |
| Counsellor, Defence Science, London | Doc Control Sheet |
| Counsellor, Defence Science, Washington | Doc Control Sheet |
| Scientific Advisor to MRDC Thailand | Doc Control Sheet |
| Director General Scientific Advisers and Trials<br>Scientific Adviser Policy and Command | 1 |
| Navy Scientific Adviser | Doc Control Sheet & Distribution List |
| Scientific Adviser, Army | Doc Control Sheet & Distribution List |
| Air Force Scientific Adviser | 1 |
| Director Trials | 1 |
| **Aeronautical and Maritime Research Laboratory** | |
| Director, Aeronautical and Maritime Research Laboratory | 1 |
| **Electronics and Surveillance Research Laboratory** | |
| Director, Electronics and Surveillance Research Laboratory | Doc Control Sheet & Distribution List |
| Chief, Information Technology Division | 1 |
| Research Leader Command & Control and Intelligence Systems | 1 |
| Research Leader Military Computing Systems | 1 |
| Research Leader Command, Control and Communications | 1 |
| Research Leader Joint Systems | 1 |
| Research Leader Advanced Computer Capabilities | Doc Control Sheet |

| | |
|---|---|
| Head, Information Warfare Studies Group | 1 |
| Head, Software Systems Engineering Group | Doc Control Sheet |
| Head, Year 2000 Project | Doc Control Sheet |
| Head, Trusted Computer Systems Group | Doc Control Sheet |
| Head, Systems Simulation and Assessment Group | 1 |
| Head, C3I Operational Analysis Group | Doc Control Sheet |
| Head, Information Management and Fusion Group | 1 |
| Head, Human Systems Integration Group | Doc Control Sheet |
| Head, C2 Australian Theatre, DSTO, HQAST, 14-18 Wylde Street, Potts Point, NSW, 2011. | 1 |
| Head, Distributed Systems Group | Doc Control Sheet |
| Head, C3I Systems Concepts Group | 1 |
| Head, Organisational Change Group | Doc Control Sheet |
| Task Manager, Mr J. G. Schapel | 1 |
| Author, Mr R. J. Staker | 4 |
| Publications and Publicity Officer, ITD<br>Executive Officer, ITD | 1 |

**DSTO Library and Archives**

| | |
|---|---|
| Library Fishermens Bend | 1 |
| Library Maribyrnong | 1 |
| Library Salisbury | 2 |
| Australian Archives | 1 |
| Library, MOD, Pyrmont | Doc Control Sheet |

**Strategic Policy and Plans Division**

| | |
|---|---|
| Director General Capability Analysis, R1-5-A054, Department of Defence, Canberra ACT 2600 | 1 |

**Capability Systems Staff**

| | |
|---|---|
| Director General Aerospace Development | Doc Control Sheet |
| Director General Maritime Development | Doc Control Sheet |
| Director General Land Development | Doc Control Sheet |
| Director General C3I Development | Doc Control Sheet |

**Headquarters Australian Theatre**

| | |
|---|---|
| J5, HQAST, 14-18 Wylde Street, Potts Point NSW 2011 | 1 |
| J6, HQAST, 14-18 Wylde Street, Potts Point NSW 2011 | 1 |
| CMDR ASTJIC, Level 5W, Maritime Headquarters, Potts Point NSW 2011 | 1 |

**Air Force**

Headquarters Air Command (*for DIW-A*), RAAF Base, Glenbrook NSW 2773 — 1

**Intelligence Program**

DGSTA, Defence Intelligence Organisation — 1

Manager, Information Centre, Defence Intelligence Organisation — 1

**Defence Information Systems Group**

Director General Corporate Information Policy and Plans, NCC-B12-WS28, Department of Defence, Canberra ACT 2600 — 1

**Finance and Inspector-General Program**

Assistant Secretary Security (*for Director of Security - Technical*), K-3-60, Department of Defence, Canberra ACT 2600 — 1

**Corporate Support Program (libraries)**

Officer in Charge, TRS, Defence Regional Library, Canberra — 1

Additional copies for DEC for exchange agreements

US Defense Technical Information Center — 2

UK Defence Research Information Centre — 2

Canada Defence Scientific Information Service — 1

NZ Defence Information Centre — 1

National Library of Australia — 1

## UNIVERSITIES AND COLLEGES

Australian Defence Force Academy Library — 1

Head of Aerospace and Mechanical Engineering, ADFA — 1

Deakin University Library, Serials Section (M List), Deakin University Library, Geelong, 3217 — 1

Senior Librarian, Hargrave Library, Monash University — 1

Librarian, Flinders University — 1

## OTHER ORGANISATIONS

NASA (Canberra) — 1

Australian Government Publishing Service — 1

The State Library of South Australia — 1

Parliamentary Library of South Australia — 1

## OUTSIDE AUSTRALIA

### ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service — 1

| | |
|---|---|
| Engineering Societies Library, US | 1 |
| Materials Information, Cambridge Science Abstracts, US | 1 |
| Documents Librarian, The Center for Research Libraries, US | 1 |
| **INFORMATION EXCHANGE AGREEMENT PARTNERS** | |
| Acquisitions Unit, Science Reference and Information Service, UK | 1 |
| Library – Exchange Desk, National Institute of Standards and Technology, US | 1 |
| **SPARES** | |
| DSTO Salisbury Research Library | 5 |
| **Total number of copies:** | 65 |

| DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION DOCUMENT CONTROL DATA | 1. CAVEAT/PRIVACY MARKING |
|---|---|

| 2. TITLE | 3. SECURITY CLASSIFICATION |
|---|---|
| Military Information Operations Analysis Using Influence Diagrams And Coloured Petri Nets | Document (U)<br>Title (U)<br>Abstract (U) |
| 4. AUTHOR(S) | 5. CORPORATE AUTHOR |
| R. J. Staker | Electronics and Surveillance Research Laboratory<br>PO Box 1500<br>Salisbury, South Australia, Australia 5108 |

| 6a. DSTO NUMBER | 6b. AR NUMBER | 6c. TYPE OF REPORT | 7. DOCUMENT DATE |
|---|---|---|---|
| DSTO–TR–0914 | AR–011–162 | Technical Report | December, 1999 |

| 8. FILE NUMBER | 9. TASK NUMBER | 10. SPONSOR | 11. No OF PAGES | 12. No OF REFS |
|---|---|---|---|---|
| N8316/21/1 | JNT 96/229 | DGISC | 72 | 17 |

| 13. DOWNGRADING / DELIMITING INSTRUCTIONS | 14. RELEASE AUTHORITY |
|---|---|
| Not Applicable | Chief, Information Technology Division |

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

*Approved For Public Release*

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE CENTRE, DIS NETWORK OFFICE, DEPT OF DEFENCE, CAMPBELL PARK OFFICES, CANBERRA, ACT 2600

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS

No Limitations

18. DEFTEST DESCRIPTORS

Military Operations
Information Warfare
Decision Making
Petri Nets

19. ABSTRACT

This report describes how Influence Diagrams, Coloured Petri Net models and related techniques may be used to analyse certain aspects of Military Information Operations. An example is employed to demonstrate these techniques. The example used is a very simplified representation of a Military Command Organisation dealing with a decision problem.

The objective of the report is to provide theory, methods and techniques to support the assessment of the effect of Military Information Operations on such organisations. The simplicity of the example permits the basic concepts to be clearly conveyed. They may readily be extended to the analysis of more complex examples as required.

The most fundamental and significant concept developed in this report is that of a common quantitative measure of effectiveness that encompasses all types of Information Operations relevant to Information Warfare. This permits the direct comparison of the effectiveness of alternative Information Operation options with one another and also with conventional operations options. This latter ability is essential if Information Operations are to be employed appropriately as part of a broader range of military options.